UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

IN RE: CHANGE HEALTHCARE, INC. CUSTOMER DATA SECURITY BREACH LITIGATION *This Document Relates To All Individual Actions*	MDL No. 24-3108 (DWF/DJF) **MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS CONSOLIDATED CLASS ACTION COMPLAINT AND MOTION TO NARROW CLASS DEFINITION**

TABLE OF CONTENTS

Page

BACKGROUND 3

LEGAL STANDARD 4

ARGUMENT 4

I. PLAINTIFFS LACK STANDING BECAUSE THEY CANNOT ALLEGE INJURY-IN-FACT OR TRAEABILITY 5

A. Several Types of Alleged Harm Fail to Confer Article III Standing 6

B. No Plaintiff Can Plausibly Allege Any Injury Is Traceable to the Cyberattack 13

II. INJURIES THAT CANNOT SUPPORT ARTICLE III STANDING SHOULD BE STRUCK & THE CLASS DEFINITONS NARROWED 16

III. PLAINTIFFS CANNOT ADEQUATELY PLEAD CAUSATION AND INJURY TO MEET RULE 12(B)(6)'S REQUIREMENTS 19

A. Alleged Fraud Without Monetary Loss Fails to State a Cognizable Injury 19

B. Allegations that Plaintiffs' PII Appeared on the Dark Web Are Insufficient 22

C. Plaintiffs Cannot Satisfy the Heightened Causation Requirements of 12(b)(6) 22

IV. PLAINTIFFS FAIL TO STATE A CLAIM AGAINST THE NON-CHANGE DEFENDANTS THAT DID NOT SUFFER THE CYBERATTACK 23

V. PLAINTIFFS' NEGLIGENCE CLAIM FAILS BECAUSE THERE IS NO DUTY, MUCH LESS BREACH OR RESULTING HARM 25

A. There Is No Common Law Duty to Safeguard Information or to Notify 25

B. There Is No Duty to Provide Uninterrupted Services 28

C. Plaintiffs Do Not Plausibly Allege Breach 30

D. The Economic Loss Rule Bars Plaintiffs' Negligence Claims in Many States 31

VI. NEGLIGENCE *PER SE* SHOULD BE DISMISSED BECAUSE IT IS NOT A RECOGNIZED CAUSE OF ACTION, IS BARRED BY THE

ECONOMIC LOSS RULE, AND CANNOT RELY ON PURPORTED HIPAA OR FTC ACT VIOLATIONS 32

VII. PLAINTIFFS' BREACH OF CONTRACT CLAIM MUST BE DISMISSED BECAUSE THEY HAVE NOT SPECIFIFED CONTRACTS, THE PRESUMPTION AGAINST THIRD PARTY BENEFICIARIES PREVAILS, AND HIPAA CANNOT FORM THE BASIS OF THEIR CLAIM 33

VIII. PLAINTIFFS' UNJUST ENRICHMENT CLAIM HAS NO MERIT .. 36

A. Unjust Enrichment Is Unavailable to Plaintiffs As a Matter Of Law 37

B. Plaintiffs Fail To Plausibly Plead the Elements of Unjust Enrichment 39

1. Plaintiffs Fail To Allege They Conferred Any Benefit to Defendants 39

2. Plaintiffs Fail To Plausibly Allege Any Enrichment Was Unjust 40

IX. THE DECLARATORY JUDGMENT ACT CLAIM IS DUPLICATIVE AND STATES NO RISK OF IMMINENT AND SUBSTANTIAL HARM 41

X. STATE CONSUMER PROTECTION CLAIMS FAIL AS PLAINTIFFS ARE NOT CONSUMERS, MADE NO PURCHASE, AND DO NOT ALLEGE UNLAWFUL OR UNFAIR CONDUCT OR INTENTIONAL DISCLOSURE 42

A. Plaintiffs Do Not Satisfy Injury and Causation Requirements 43

B. Plaintiffs Are Not Consumers and Made No Purchases from Defendants 45

C. Plaintiffs Failed to Satisfy Statutory Notice Requirements 45

D. Plaintiffs Seek Relief Beyond What Is Authorized By Statutes 46

E. Defendants Did Not Engage in Unlawful or Unfair Conduct 47

1. No Unlawful Conduct Under HIPAA, FTC Act, or Other Statutes 48

2. Plaintiffs Have Not Shown Egregious or Aggravating Circumstances 49

F. Plaintiffs Cannot Satisfy the Requirements of Information Statutes 51

1. There is No Intentional Disclosure of Medical Information Under California Confidentiality of Medical Information Act ("CMIA") (Count XII)..... 51

2. The Minnesota Health Records Act ("MHRA") (Count XXV) Claim Fails Because Plaintiffs Do Not Allege A Release of Health Records 52

3. The Wisconsin Health Care Records Law ("WHCRL") (Count XL) Claim Fails As Plaintiff Cannot Allege Disclosure or Resulting Harm 53

XI. DATA BREACH NOTIFICATION CLAIMS FAIL BECAUSE PLAINTIFFS DO NOT ALLEGE UNREASONABLE DELAY OR HARM 53

CONCLUSION..... 56

TABLE OF AUTHORITIES

Page(s)

Cases

Ahlgren v. Muller,
438 F. Supp. 3d 981 (D. Minn. 2020) 38

Alberts v. Payless Shoesource, Inc.,
No. 13-12262,
2014 WL 4924243 (D. Mass. Sept. 29, 2014) 46

ALK 2, LLC v. K2 Marine, Inc.,
647 F. Supp. 3d 1253 (M.D. Ala. 2022) 45

Amusement Indus., Inc. v. Stern,
693 F. Supp. 2d 301 (S.D.N.Y. 2010) 42

Arena Holdings Charitable, LLC v. Harman Prof'l, Inc.,
785 F.3d 292 (8th Cir. 2015) 31

Ashcroft v. Iqbal,
556 U.S. 662 (2009) 4, 8, 40, 41, 51

Aspen Am. Ins. Co. v. Blackbaud, Inc.,
No. 3:22-CV-44,
2023 WL 3737050 (N.D. Ind. May 31, 2023) 25, 27

Attias v. CareFirst, Inc.,
365 F. Supp. 3d 1 (D.D.C. 2019) 26

Beck v. McDonald,
No. 19-2814, 848 F.3d 262 (4th Cir. 2017) 8, 9

Bell Atl. Corp. v. Twombly,
550 U.S. 544 (2007) 4

Bergman v. Spruce Peak Realty, LLC,
847 F.Supp.2d 653 (D. Vt. 2012) 48

Bonewit v. New-Indy Containerboard LLC,
No. 24-cv-11338,
2024 WL 4932186 (D. Mass. Dec. 2, 2024) 22

Brickman v. Maximus, Inc.,
No. 2:21-cv-3822,
2023 WL 2563661 (S.D. Ohio Mar. 17, 2023) 31

Bricks, Inc. v. BNY Tr. Co. of Missouri,
165 F. Supp. 2d 723 (W.D. Tenn. 2001) 33

Broder v. Cablevision Sys. Corp.,
418 F.3d 187 (2d Cir. 2005) 48

Brown v. Medtronic, Inc.,
628 F.3d 451 (8th Cir. 2010) 19

Bruno v. Donohoe as Tr. of Texas Med. Liab. Tr.,
No. 1:23-CV-01183,
2024 WL 5305079 (W.D. Tex. Oct. 25, 2024) 33, 35

Buchl v. Gascoyne Materials Handling & Recycling, L.L.C.,
No. 1:17-CV-48,
2018 WL 3259740 (D.N.D. Mar. 21, 2018) 38

Burger v. Healthcare Mgmt. Sols., LLC,
No. 23-1215,
2024 WL 473735 (D. Md. Feb. 7, 2024) 11,

C.C. v. Med-Data Inc.,
No. 21-2301,
2022 WL 970862 (D. Kan. Mar. 31, 2022) 9

Caldas v. Affordable Granite & Stone, Inc.,
820 N.W.2d 826 (Minn. 2012) 33, 36, 38, 39

CarMax Auto Superstores Inc. v. Sibley,
194 F. Supp. 3d 392 (D. Md. 2016) 48

Cellco P'ship v. Hope,
No. CV11-0432 PHX,
2011 WL 3159172 (D. Ariz. July 26, 2011) 45

Chambliss v. CareFirst, Inc.,
189 F. Supp. 3d 564 (D. Md. 2016) 11

Clapper v. Amnesty Int'l USA,
568 U.S. 398 (2013) 5, 8

Clemens v. ExecuPharm Inc.,
48 F.4th 146 (3d Cir. 2022) 7

Cmty. Bank of Trenton v. Schnuck Mkts., Inc.,
No. 15-cv-01125,
2017 WL 1551330 (S.D. Ill. May 1, 2017) 27

Cmty. Bank of Trenton v. Schnuck Mkts., Inc.,
887 F.3d 803 (7th Cir. 2018) 31

Coletti, et al. v. Change Healthcare, Inc.,
No. 0:24-cv-03681(D. Minn. opened Sept. 17, 2024) 14, 15

Crowe v. Managed Care of N. Am.,
No. 0:23-cv-61065-AHS (S.D. Fla. Opened June 5, 2023) 30

Dep't of Labor v. McConnell,
828 S.E.2d 352 (Ga. 2019) 25

Dias v. Spartan Micro, Inc.,
No. 8:22-cv-00834,
2022 WL 17216820 (C.D. Cal. Sept. 14, 2022) 37

Dickerson v. Colonial Pipeline Co.,
No. 1:21-CV-2098,
2022 WL 18717801 (N.D. Ga. June 17, 2022) 28, 29

Donelson v. Ameriprise Fin. Servs. Inc.,
999 F.3d 1080 (8th Cir. 2021) 16, 18

Dorosh v. Minn. Dep't of Hum. Servs.,
No. 23-cv-1144,
2023 WL 6279374 (D. Minn. Sept. 26, 2023) 24

Edwards v. Zenimax Media Inc.,
No. 12-cv-00411,
2012 WL 4378219 (D. Colo. Sept. 25, 2012) 17

Elsherif v. Mayo Clinic,
No. 18-2998,
2019 WL 1505960 (D. Minn. Apr. 5, 2019) 34

Espinoza v. Gold Cross Servs., Inc.,
234 P.3d 156 (Utah Ct. App. 2010) 37

Fairview Health Servs. V. Armed Forces Off. Of Royal Embassy of Saudi Arabia,
705 F. Supp. 3d 898 (D. Minn. 2023) 42

Fernandez v. Leidos, Inc.,
127 F. Supp. 3d 1078 (E.D. Cal. 2015) 11

Fero v. Excellus Health Plan, Inc.,
236 F. Supp. 3d 735 (W.D.N.Y. 2017) 48

Fraga v. UKG Inc.,
No. 22-20105-CIV,
2022 WL 19486310 (S.D. Fla. May 10, 2022) 11

Freeman Indus., LLC v. Eastman Chem. Co.,
172 S.W.3d 512 (Tenn. 2005) 37, 40

George D. v. NCS Pearson, Inc.,
No. 19-2814,
2020 WL 3642325 (D. Minn. July 6, 2020) 9

Gilbert v. United States Olympic Comm.,
423 F. Supp.3d 1112, 1155 (D. Colo. 2019) 17

Gilbert v. United States Olympic Comm.,
No. 18-cv-00981,
2019 WL 1058194 (D. Colo. Mar. 6, 2019) 17

Gisairo v. Lenovo (United States) Inc.,
516 F. Supp. 3d 880 (D. Minn. 2021) 46

Gorman v. Ethos Grp. Inc.,
No. 3:22-cv-02573-M,
2024 WL 1257493 (N.D. Tex. Mar. 25, 2024) 25

Griffey v. Magellan Health Inc.,
No. CV-20-01282-PHX,
2022 WL 1811165 (D. Ariz. June 2, 2022) 45

Guthrie v. Bank of Am., Nat'l Ass'n,
No. CIV. 12-2472,
2012 WL 6552763 (D. Minn. Dec. 14, 2012) 32

Halvorson v. Auto-Owners Ins. Co.,
718 F.3d 773 (8th Cir. 2013) 4, 16

Hamilton v. Palm,
621 F.3d 816 (8th Cir. 2010) 21

Harris v. Nationwide Mut. Fire Ins. Co.,
367 F. Supp. 3d 768 (M.D. Tenn. 2019) 26

Haywood v. Novartis Pharms. Corp.,
298 F. Supp. 3d 1180 (N.D. Ind. 2018) 26

Hollingsworth v. Perry,
570 U.S. 693 (2013) 43

Hovsepian v. Apple, Inc.,
No. 08-5788 (PVT),
2009 WL 5069144 (N.D. Cal. Dec. 17, 2009) 18

Hubbard v. Google LLC,
No. 19-cv-07016,
2024 WL 3302066 (N.D. Cal. July 1, 2024) 11, 12

In re Accellion, Inc. Data Breach Litig.,
713 F. Supp. 3d 623 (N.D. Cal. 2024) 50

In re: Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.,
No. 19-md-2904,
2021 WL 5937742 (D.N.J. Dec. 16, 2021) 51

In re Anthem, Inc. Data Breach Litig.,
No. 15-MD-02617,
2016 WL 3029783 (N.D. Cal. May 27, 2016) 36

In re Arthur J. Gallagher Data Breach Litig.,
631 F. Supp. 3d 573 (N.D. Ill. 2022) 39

In re Blackbaud, Inc., Customer Data Breach Litig.,
No. 3:20-mn-02972,
2024 WL 2155221 (D.S.C. May 14, 2024) 17

In re Ductile Iron Pipe Fitting Indirect Purchaser Antitrust Litig.,
No. 12-169,
2013 WL 5503308 (D.N.J. Oct. 2, 2013) 42

In re Ford Motor Co. F-150 & Ranger Truck Fuel Econ. Mktg. & Sales Pracs. Litig.,
No. 2:19-md-02901,
2022 WL 551221 (E.D. Mich. Feb. 23, 2022) 47

In re iPhone Application Litig.,
No. 11-MD-02250,
2011 WL 4403963 (N.D. Cal. Sept. 20, 2011) 43

In re LastPass Data Sec. Incident Litig.,
742 F. Supp. 3d 109 (D. Mass. 2024) 26

In re LinkedIn User Priv. Litig.,
932 F.Supp. 2d 1089 (N.D. Cal. 2013) 11

In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig.,
341 F.R.D. 128 (D. Md. 2022) 17

In re MCG Health Data Sec. Issue Litig.,
No. 2:22-CV-849,
2023 WL 3057428 (W.D. Wash. Mar. 27, 2023) 39, 49

In re MCG Health Data Sec. Issue Litig.,
No. 2:22-CV-849,
2023 WL 4131746 (W.D. Wash. June 22, 2023) 50

In re: Michaels Stores Pin Pad Litig.,
830 F. Supp. 2d 518 (N.D. Ill. 2011) 20

In re: Netgain Tech. LLC, Customer Data Breach Litig.,
No. 21-cv-1210,
2022 WL 1810606 (D. Minn. June 2, 2022) 52

In re: Practicefirst Data Breach Litig.,
No. 21-CV-790,
2022 WL 3045319 (W.D.N.Y. Aug. 1, 2022) 9

In re: Practicefirst Data Breach Litig.,
No. 1:21-CV-00790,
2022 WL 354544 (W.D.N.Y. Feb. 2, 2022) 9, 10, 13

In re: Samsung Data Sec. Breach Litig.,
No. 1:23-md-03055,
2025 WL 271059 (D.N.J. Jan. 3, 2025) 6, 8, 11

In re St. Jude Med. Inc. Silzone Heart Valves Prods. Liab. Litig.,
MDL No. 01-1396,
2009 WL 1789376 (D. Minn. June 23, 2009) 4

In re SuperValu Customer Data Sec. Breach Litig.,
No. 14-MD-2586,
2016 WL 81792 (D. Minn. Jan. 7, 2016) 11

In re: SuperValu, Inc., Customer Data Sec. Breach Litig.,
870 F.3d 763 (8th Cir. 2017) 6, 7, 8, 11, 19

In re SuperValu, Inc., Customer Data Sec. Breach Litig.,
925 F.3d 955 (8th Cir. 2019) 4, 19, 25, 38, 41, 43, 44

In re: SuperValu, Inc., Customer Data Sec. Breach Litig.,
No. 14-MD-2586,
2018 WL 1189327 (D. Minn. Mar. 7, 2018) 19, 20, 22

In re Yahoo! Inc. Customer Data Sec. Breach Litig.,
No. 16-MD-02752,
2017 WL 3727318 (N.D. Cal. Aug. 30, 2017) 43

In re Zappos.com, Inc. Customer Data Sec. Breach Litig.,
108 F. Supp. 3d 949 (D. Nev. 2015) 9

Insulate SB, Inc. v. Advanced Finishing Sys., Inc.,
No. 13-2664,
2014 WL 943224 (D. Minn. Mar. 11, 2014) 42, 52

Irwin v. Jimmy John's Franchise,
175 F. Supp. 3d. 1064 (C.D. Ill. 2016) 39

Jenkins v. Assoc. Wholesale Grocers, Inc.,
No. 24-4039,
2025 WL 708574 (D. Kan. Mar. 5, 2025) 6, 12, 13, 14

Kilpatrick v. Bryant,
868 S.W.2d 594 (Tenn. 1993) 23

Kuchenmeister v. HealthPort Techs., LLC,
753 F. App'x 794 (11th Cir. 2018) 35

Langbehn v. Pub. Health Tr. of Miami-Dade Cnty.,
661 F. Supp. 2d 1326 (S.D. Fla. 2009) 33

Larson v. Nw. Mut. Life Ins. Co.,
855 N.W.2d 293 (Minn. 2014) 52

Lochridge v. Quality Temp. Servs., Inc.,
No. 22-cv-12086,
2023 WL 4303577 (E.D. Mich. June 30, 2023) 41

Lujan v. Defs. of Wildlife,
504 U.S. 555 (1992) 5

Lyons v. Bank of Am., NA,
No. C 11-1232,
2011 WL 6303390 (N.D. Cal. Dec. 16, 2011) 17

Madrid v. Perot Sys. Corp.,
130 Cal. App. 4th 440 (Cal. Ct. App. 3d 2005) 46

Malone v. Norwest Fin. Cal. Inc.,
245 B.R. 389 (E.D. Cal. 2000) 27

Manigault-Johnson v. Google, LLC,
No. 2:18-cv-1032,
2019 WL 3006646 (D.S.C. Mar. 31, 2019) 23

Manley v. Experian Data,
No. 4:21-CV-00199,
2021 WL 9274364 (N.D. Ga. Dec. 13, 2021) 54

Miller v. NextGen Healthcare, Inc.,
742 F. Supp. 3d 1304 (N.D. Ga. 2024) 54

Minneapolis Cablesystems v. City of Minneapolis,
299 N.W.2d 121 (Minn. 1980) 34

Mosley v. Oakwood Lutheran Senior Ministries,
No. 2022AP907,
2023 WL 4782874 (Wis. Ct. App. July 27, 2023) 53

Murray v. ILG Techs., LLC,
798 F. App'x 486 (11th Cir. 2020) 29

Nelson v. Ashford Univ., LLC,
No. 16-cv-3491,
2016 WL 4530325 (N.D. Ill. Aug. 29, 2016) 43

Ojogwu v. Rodenburg L. Firm,
26 F.4th 457 (8th Cir. 2022) 12

Olsen v. Johnston,
301 P.3d 791 (Mont. 2013) 34

Owens v. Rodale, Inc.,
No. 14-12688,
2015 WL 575004 (E.D. Mich. Feb. 11, 2015) 35

Partin v. Baptist Healthcare Sys., Inc.,
No. 4:20-cv-00185,
2022 WL 10078122 (S.D. Ind. Oct. 17, 2022) 34

Patterson v. Med. Rev. Inst. of Am., LLC,
No. 22-cv-00413,
2022 WL 2267673 (N.D. Cal. June 23, 2022) 13

Pennell v. Glob. Tr. Mgmt, LLC,
990 F.3d 1041 (7th Cir. 2021) 12

Pirozzi v. Apple, Inc.,
913 F. Supp. 2d 840 (N.D. Cal. 2012) 25

Pisciotta v. Old Nat'l Bancorp,
499 F.3d 629 (7th Cir. 2007) 27

RBG Mgmt. Corp. v. Vill. Super Mkt., Inc.,
692 F. Supp. 3d 135 (S.D.N.Y. 2023) 40

Reilly v. Ceridan Corp.,
664 F.3d 38 (3d Cir. 2011) 8

Robbins v. Perry Cnty.,
No. M2008-00548-COA-R3-CV,
2009 WL 1162579 (Tenn. Ct. App. 2009) 23

Rodi v. S. New Eng. Sch. of L.,
389 F.3d 5 (1st Cir. 2004) 46

Rogers v. Keffer, Inc.,
243 F. Supp. 3d 650 (E.D.N.C. 2017) 55

S. Bay Chevrolet v. Gen. Motors Acceptance Corp.,
72. Cal. App. 4th 47

Sanders v. Apple Inc.,
672 F. Supp.2d 978 (N.D. Cal. 2009) 18

Sheldon v. Kettering Health Network,
40 N.E.3d 661 (Ohio Ct. App. 2015) 26

Smahaj v. Retrieval-Masters Creditors Bureau, Inc.,
131 N.Y.S.3d 817 (N.Y. Sup. Ct. 2020) 25

Smith v. AVSC Int'l, Inc.,
148 F. Supp. 2d 302 (S.D.N.Y. 2001) 24

Spokeo, Inc. v. Robins,
578 U.S. 330 (2016) 5, 52

Sutter Health v. Super. Ct. Sacramento Cnty.,
227 Cal. App. 4th 1546 (Cal. Ct. App. 2014) 51

Tahirou v. New Horizon Enters., LLC,
No. 3:20-CV-0281,
2022 WL 596741 (D. Conn. Feb. 28, 2022) 38

Tate v. EyeMed Vision Care, LLC,
No. 1:21-cv-36,
2023 WL 6384367 (S.D. Oh. Sept. 29, 2023) 47

Taylor v. UKG, Inc.,
693 F.Supp.3d 87 (D. Mass. 2023) 9

Tietsworth v. Sears,
720 F.Supp.2d 1123 (N.D. Cal. Mar. 31, 2010) 18

Topchian v. JPMorgan Chase Bank, N.A.,
760 F.3d 843 (8th Cir. 2014) 21

TransUnion LLC v. Ramirez,
594 U.S. 413 (2021) 21

Travelers Indem. Co. v. Dammann & Co.,
594 F.3d 238 (3d Cir. 2010) 29

Trone Health Servs., Inc. v. Express Scripts Holding Co.,
974 F.3d 845 (8th Cir. 2020) 32

Troy v. Am. Bar Ass'n,
No. 23-CV-03053,
2024 WL 1886753 (E.D.N.Y. Apr. 30, 2024) 48

Tureen v. Equifax, Inc.,
571 F.2d 411 (8th Cir. 1978) 9

United States v. Bestfoods,
524 U.S. 51 (1998) 23, 24

Walker v. Hixson Autoplex of Monroe, L.L.C.,
240 So. 3d 1088 (La. Ct. App. 2017) 49

Whalen v. Michael Stores Inc.,
153 F. Supp. 3d 577 (E.D.N.Y. 2015) 9

Williams v. Bienville Orthopaedic Specialists, LLC,
737 F. Supp. 3d 411 (D. Miss. 2024) 12

Zean v. Fairview Health Services,
858 F.3d 520 (8th Cir. 2017) 3, 15

Statutes

42 U.S.C. § 1320d-6(a) 32

Alaska Stat. § 45.48.010 56

Alaska Stat. § 45.48.070 56

Cal. Civ. Code § 1798.82(a)-(b) 56

Cal. Civ. Code §§ 1798.145(c)(1)(A)-(B) 47

California Consumer Privacy Act, Cal. Civ. Code § 1798.150(b) 45, 48

Declaratory Judgment Act, 28 U.S.C. § 2201 41

Georgia Identity Theft Protection Act, Ga. Code Ann. § 10-1-910 (2024) 54

Maryland Social Security Number Privacy Act, Md. Code Ann. Comm. L.
§ 14-3401, *et seq*. 48

Md. Code Ann. Comm. L. § 14-3402(a)(1) 49

Md. Code Ann. Comm. L. § 14-3402(a)(2) 49

Md. Code Ann. Comm. L. § 14-3402(a)(4) 49

Minnesota Health Records Act, Minn. Stat. Ann. § 144.291 subdiv. 2(c) 52

S.C. Code Ann. § 39-1-90(A) 56

S.C. Code Ann. § 39-1-90(B) 54, 56

Wash. Rev. Code § 19.255.010(1)-(2) 56

Wis. Stat. § 146.81(4) 53

Wis. Stat. § 146.82(1) 53

Wis. Stat. § 146.84(1)(bm) 53

Rules

Fed. R. Civ. P. 8(a) 19, 24, 34

Fed. R. Civ. P. 9(b) 48

Fed. R. Civ. P. 12(b)(6) 19, 22

Fed. R. Civ. P. 12(f) 17

Fed. R. Civ. P. 23(d)(1)(D) 4, 16, 17

Other Authorities

Responses to Questions for the Record for Andrew Witty, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/responses_for_questions_for_the_record_to_andrew_witty.pdf (last visited Mar. 21, 2025) 10

Early last year, Change Healthcare ("Change") was the victim of a sophisticated criminal ransomware attack (the "Cyberattack"). Change is not unique in suffering such an incident—there are hundreds of successful attacks against companies annually. But Change's response, protecting the broader healthcare system and prioritizing continuity of care, was unprecedented. In addition to swiftly securing its network and paying the ransom to stop the data from being made public, Change loaned ***$9 billion*** to healthcare providers to ensure patients did not feel an impact from Change's decision to contain the breach. Change also offered everyone, regardless of whether their information was impacted or even held by Change, two years of free credit monitoring and identity protection services.

Against this backdrop, Plaintiffs—individuals nationwide who allege their data was impacted in the incident—bring suit built on a flawed premise and seek to manufacture liability where there is none. As Plaintiffs see it, *because* Change fell victim to the Cyberattack, Defendants must have been negligent. But negligence is not strict liability, and the mere occurrence of a cyberattack does not establish duty, breach, or injury—all of which must be plausibly pled to survive a motion to dismiss. Plaintiffs' effectively-*per se* theory of liability runs contrary to hundreds of years of common law precedent and dozens of more recent applications in breach cases. It also disregards the facts as pled. In Plaintiffs' own telling, Defendants *had* reasonable data security, as they were "constantly assessing and improving capabilities, working with key technology partners, sharing information about security threats and best practices, [and] running continuous penetration tests" and working to strengthen cybersecurity at the time of the Cyberattack. The unfortunate reality

is that companies can maintain robust cybersecurity practices, work toward remediating vulnerabilities, and still be victimized by ransomware gangs—that is not negligence.

Plaintiffs use the same faulty foundation to prop up the rest of their common law claims and many of their statutory claims. For instance, Plaintiffs cannot point to any contract that can be breached by the mere occurrence of a cyberattack, nor can they articulate how suffering such an attack has resulted in Defendants' enrichment, much less unjustly. Similar failures trickle down through Plaintiffs' statutory claims, many of which are ill-suited or inapplicable where no consumer transaction occurred, and others of which require "reasonable" data security—not an absolute duty to never suffer a cyber incident.

The failures of the Complaint persist as to whether the Plaintiffs even have standing to bring their claims. They do not. Plaintiffs are either uninjured or can only speculate they might—or might not—face future injury. Plaintiffs' insistence of their harm is hard to square with their acknowledgment that Defendants acted swiftly to secure the data and paid a ransom to protect it. To be sure, Plaintiffs allege a host of harms common to the inconveniences of modern life: spam text messages, the existence of data on the dark web, and *attempted* fraudulent transactions. But they cannot tie those purported harms to *this* incident, as opposed to one of the 1,000 other cyberattacks attributed to this perpetrator alone, to say nothing of the thousands of other cyberattacks in the last decade.

The CAC should be dismissed.

BACKGROUND

UnitedHealth Group Incorporated ("UHG") operates with a mission "to help people live healthier lives and help make the health system work better for everyone."[1] CAC ¶ 212 n.77. In 2022, UHG acquired Change, which transmits information, claims, and payments between physicians, health plans, and other third parties. *Id.* ¶¶ 4, 212 n.77. Plaintiffs also bring claims against Optum, Inc. and OptumInsight, Inc., UHG subsidiaries. *See, e.g.*, *id.* ¶ 527.

The Cyberattack on Change was perpetrated by sophisticated criminal threat actors whose resources were focused on going undetected. *Id.* ¶¶ 254-57. The system leveraged by the attackers was not sensitive, and it was only because of the attackers' savvy techniques that they were able to move beyond that system to other systems. *Id.* ¶¶ 212; 251 (stating the compromised account did not have administrator access); *id.* ¶ 254 (explaining the criminals "moved laterally within [Change's] systems in more sophisticated ways" and "created privileged accounts"). The Cyberattack was limited to Change's environment. *Id.* ¶ 259. Defendants took swift action to contain the Cyberattack, including by: isolating and disconnecting Change's systems to prevent impact to providers, patients, and other individuals and entities, *id.* ¶¶ 212 n.77, 258, 274; retaining security experts and

[1] The Court may consider the statements made on this website, which was cited in the CAC, without converting this Motion into a Motion for Summary Judgment, because it is a "document[] whose contents are alleged in a complaint and whose authenticity no party questions." *Zean v. Fairview Health Services*, 858 F.3d 520, 526 (8th Cir. 2017).

working with law enforcement, *id.* ¶ 258; promptly paying a ransom to protect consumers and Change's customers, *id.* ¶ 11; and rebuilding Change's systems, *id.* ¶ 212 n.77.

LEGAL STANDARD

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *In re SuperValu, Inc.*, *Customer Data Sec. Breach Litig.,* 925 F.3d 955, 962 (8th Cir. 2019) (*SuperValu IV*) (internal quotations omitted). A claim is plausible only when the plaintiff "pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The plaintiff must allege "more than a sheer possibility that a defendant has acted unlawfully." *Id.* Factual allegations must be "more than labels and conclusions" or "a formulaic recitation of the elements of a cause of action." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

Rule 23(d)(1)(D) allows a court to "issue orders that . . . require that the pleadings be amended to eliminate allegations about representation of absent persons." This includes the authority to strike particular class allegations if they are "insufficient to satisfy the requirements for certification." *In re St. Jude Med. Inc. Silzone Heart Valves Prods. Liab. Litig.*, MDL No. 01-1396 (JRT/FLN), 2009 WL 1789376, at *2 (D. Minn. June 23, 2009). In the Eighth Circuit, each member of a class "must have standing and show an injury in fact." *Halvorson v. Auto-Owners Ins. Co*., 718 F.3d 773, 778 (8th Cir. 2013).

ARGUMENT

Defendants move to dismiss the CAC for lack of standing and failure to state a claim. Specifically, certain Plaintiffs fail to show a concrete injury-in-fact that is traceable

to any Defendant's conduct, as required to confer Article III standing. Since certain alleged injuries on their own are never sufficient to confer standing, Defendants also move to modify the class definitions accordingly. Beyond standing, Plaintiffs fail to allege both a cognizable injury and a causal connection between the Cyberattack and any purported harm, required elements cutting across all claims. Finally, Plaintiffs' common law and statutory claims fail for myriad reasons, requiring dismissal of the CAC in its entirety.

I. PLAINTIFFS LACK STANDING BECAUSE THEY CANNOT ALLEGE INJURY-IN-FACT OR TRACEABILITY

Plaintiffs Agres, Antonio, Hanes, Johnson, Kentner, Lovell, Schwalbe, and Seibert (the "No Injury Plaintiffs"), lack Article III standing because they fail to allege facts sufficient to show an injury that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992); *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013). A plaintiff invoking the Court's jurisdiction can only demonstrate standing by showing that she has suffered an injury-in-fact that is fairly traceable to the defendant's conduct and that is likely to be redressed by the relief sought. *Clapper*, 568 U.S. at 409; *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016).

At bottom, the No Injury Plaintiffs simply do not allege harms sufficient to confer standing, having alleged only purported injuries like receipt of spam calls and time spent researching the Cyberattack or monitoring related to the same. *See* CAC ¶¶ 43-44, 66-67, 84-87, 126-27, 132-37. While all Plaintiffs collectively allege that they have suffered

diminution or lost value of their data and emotional distress,[2] as addressed below, each of these so-called injuries fall short of satisfying Article III on their own and should be struck. *See, e.g.*, *In re: Samsung Data Sec. Breach Litig.*, No. 1:23-md-03055, 2025 WL 271059, at *11 (D.N.J. Jan. 3, 2025) (dismissing data breach case because actions in anticipation of speculative, potential future harm do not satisfy the injury-in-fact requirement).

Even plaintiffs who assert Article III injury at this phase (*i.e.*, the Plaintiffs outside of the No Injury Plaintiffs) cannot show that any alleged harm is traceable to *this* incident, as opposed to the 1,000+ other attacks attributed to this threat actor alone. CAC ¶ 238; *see also, e.g.*, *Jenkins v. Assoc. Wholesale Grocers, Inc.*, No. 24-4039, 2025 WL 708574, at *7-8 (D. Kan. Mar. 5, 2025) (dismissing claim despite fraudulent charges because plaintiff could not allege "PII disclosed in *this* data breach was misused").

A. Several Types of Alleged Harm Fail to Confer Article III Standing

No Substantial Risk of Future Harm. The aptly named No Injury Plaintiffs primarily rely upon risk of *future* harm as the basis for their purported injury-in-fact. *See In re: SuperValu, Inc., Customer Data Sec. Breach Litig.*, 870 F.3d 763, 769-72 (8th Cir. 2017) (*SuperValu II*). This is not enough for injury under Article III.

[2] Plaintiffs *collectively* allege ten categories of purported injuries: (1) loss of privacy; (2) misappropriation of their identity; (3) fraud and identity theft; (4) diminution in the value of their data; (5) loss of value in their data; (6) emotional distress; (7) disruption in medical care; (8) disruption in pharmaceutical access; (9) lost time, effort, and expense; and (10) risk of misuse of their data. *See, e.g.*, CAC ¶ 15. This generic, group pleading lays bare that these injuries are not concrete or particularized as to any Plaintiff and should be dismissed.

In *SuperValu II* (a data breach suit), the Eighth Circuit held that only the single plaintiff who alleged actual present-day financial harm—fraudulent credit charges—had standing. *Id.* at 767. The No Injury Plaintiffs do not make any such allegations. Instead, these Plaintiffs try to clear Article III's hurdle by pointing to a risk of future harm and other non-justiciable harms addressed below. But that risk, like in *SuperValu II,* is not sufficient to confer standing under these facts. Plaintiffs admit that Defendants paid a ransom to prevent the disclosure of data. CAC ¶ 11. Plaintiffs also do not articulate how medical information—even if it was impacted—could be used to "open unauthorized accounts in the plaintiffs' names… [or] commit credit or debit card fraud." *SuperValu II*, 870 F.3d at 770. And, in any event, no Plaintiff has plausibly alleged that they experienced any harm caused by "medical identity theft," CAC ¶ 317, and the No Injury Plaintiffs cannot articulate, therefore, why that risk might exist for them here.

At bottom, the No Injury Plaintiffs' risk of future harm allegations fail, as do any allegations they seek to borrow from their co-plaintiffs in an effort to prop up their claims. *Supervalu II*, 870 F.3d at 769-74 (refusing to impute plaintiff's alleged financial injury to buttress the non-existent standing claims of his 15 co-plaintiffs); *see also Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 153 n.4 (3d Cir. 2022) (refusing to extend one plaintiff's alleged injuries from a data breach to the analysis of other plaintiffs or class members). Consistent with *SuperValu II*, the Court must consider the risk of future injury on a plaintiff-by-plaintiff basis and find that the No Injury Plaintiffs lack Article III standing.

Mitigation Efforts. Nearly every Plaintiff alleges that they lost time or spent money "responding to" the Cyberattack because they "research[ed]" it, took other steps to "review accounts," or undertook similar proactive measures, regardless of whether or not they experienced any attempted fraud or misuse. *See, e.g.*, CAC ¶ 43 (alleging 5 hours responding to the Cyberattack, but no fraud or misuse). Plaintiffs cannot create a concrete injury by spending time working to "prevent against" speculative future harm. *Clapper,* 568 U.S. at 402. The CAC asserts that future fraud and identity theft are "inevitable," CAC ¶ 325, but this is a legal conclusion. *See Iqbal*, 556 U.S. at 678. Indeed, the CAC was filed eleven months after the Cyberattack and the No Injury Plaintiffs could not point to any instances of fraud, identity theft, or even *potential* instances of fraud or identity theft. CAC ¶¶ 43, 66, 84, 86, 126, 132, 134, 136. Courts routinely reject theories of harm in data breach cases that depend on future risk because the possibility that Plaintiffs' data will be misused by an unknown, third party at some point is conjectural. *See SuperValu II*, 870 F.3d at 771 (upholding dismissal of plaintiffs for lack of standing because the risk of future identity theft was too speculative); *Reilly v. Ceridan Corp.*, 664 F.3d 38, 42 (3d Cir. 2011) (same).

Plaintiffs' allegations of lost time researching the Cyberattack, and similar mitigation efforts, are the types of harms that courts have held are insufficient.[3] *See, e.g.*, *In re Samsung*, 2025 WL 271059, at *10-11 (collecting cases and dismissing plaintiffs for

[3] Several Plaintiffs allege more attenuated or avoidable costs, such as the cost of gasoline to drive to a police station to file a report, CAC ¶ 120, or of enrolling in credit monitoring services in addition to the service offered by Defendants for free, *id.* ¶ 90. Like lost time or credit monitoring costs, these self-generated expenses responding to a non-imminent threat of future injury cannot support Article III standing. *See Beck,* 848 F.3d at 276.

lack of standing because time and money spent to monitor accounts could not confer standing); *Beck v. McDonald*, No. 19-2814 (JRT/KMM), 848 F.3d 262, 276-77 (4th Cir. 2017) (dismissing case because costs incurred due to "fear of future identity theft based on" data breach failed to establish standing); *George D. v. NCS Pearson, Inc.*, No. 19-2814, 2020 WL 3642325, at *3 (D. Minn. July 6, 2020) (dismissing case because "time and costs associated with dealing with the data breach" are insufficient to establish standing); *Whalen v. Michael Stores Inc.*, 153 F. Supp. 3d 577, 583 (E.D.N.Y. 2015) (dismissing case because mitigation costs in response to data breach did not confer standing).

Loss of Privacy Allegations. No Plaintiff, including the No Injury Plaintiffs, can allege a loss of privacy injury, which requires disclosure of private information to the public rather than "a single person or even a small group of persons." *See Tureen v. Equifax, Inc.*, 571 F.2d 411, 417 (8th Cir. 1978). In the data breach context, courts hold that loss of privacy—even when data is exfiltrated—does not confer standing. *See, e.g.*, *Taylor v. UKG, Inc.*, 693 F.Supp.3d 87, 100-01 (D. Mass. 2023) (data exfiltration, without further evidence of publication, did not satisfy requirements for injury-in-fact). Even if Plaintiffs claim their data is available to the public, they must still plead some sort of "concrete or particularized injury associated with the disclosure." *In re: Practicefirst Data Breach Litig.*, No. 1:21-CV-790, 2022 WL 354544, at *8 (W.D.N.Y. Feb. 2, 2022), *R. & R. adopted*, No. 21-CV-790, 2022 WL 3045319 (W.D.N.Y. Aug. 1, 2022); *see also C.C. v. Med-Data Inc.,* No. 21-2301, 2022 WL 970862, at *9-10 (D. Kan. Mar. 31, 2022); *In re Zappos.com, Inc. Customer Data Sec. Breach Litig.*, 108 F. Supp. 3d 949, 962 (D. Nev. 2015) (same).

Not so here. At most, Plaintiffs describe the threat actors' extortion efforts and a dark web "experiment" with "phony" data that they suggest "demonstrated that data released on the dark web will quickly spread around the world," but notably they *do not* allege that the corpus of data exfiltrated from Change was made available on the dark web, or that it was downloaded.[4] CAC ¶¶ 276, 295. Moreover, no Plaintiff alleges a harm related to any alleged exposure of their information; the closest they come is two Plaintiffs who allege fear about "the potential impact" if certain medical history information was retained by Change, impacted in the Cyberattack, and is one day "released."[5] This is insufficient for the concrete injury needed to plead loss of privacy or misappropriation. *See, e.g.*, *In re: Practicefirst*, 2022 WL 354544, at *8 (dismissing case for lack of standing because release of information, even PHI, without an articulated injury, did not establish standing).

Lost Value or Benefit of the Bargain Theory. No Plaintiffs allege facts to support a lost value of data or lost benefit of the bargain theory.[6] These theories are "consistently rejected in data breach cases where plaintiffs have not alleged that the value of the goods or services they purchased was diminished as a result of the data breach." *In re SuperValu*

[4] Plaintiffs' reference to UHG responses to questions from a Senate Committee to suggest that data exfiltrated during the Cyberattack was posted on the dark web before the ransom was paid is misleading. CAC ¶ 276. That source confirms that the threat actor posted 22 screenshots, allegedly from exfiltrated files, for a brief period of time and that no further publication of PII or PHI had occurred. *Id.* (citing *Responses to Questions for the Record for Andrew Witty*, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/responses_for_questions_for_the_record_to_andrew_witty.pdf (last visited Mar. 21, 2025). Plaintiffs also define the dark web as "hidden" websites that "do not advertise their existence." CAC ¶ 293.

[5] *See* CAC ¶ 49; *see also id.* ¶ 76.

[6] *See* CAC ¶¶ 43-44, 66-67, 84-87, 126-27, 132-37.

Customer Data Sec. Breach Litig., No. 14-MD-2586, 2016 WL 81792, at *8 (D. Minn. Jan. 7, 2016) (*SuperValu I*) (dismissing claim based on lost benefit of the bargain because plaintiffs did not allege a data breach diminished the value of the goods they purchased), *rev'd on other grounds, SuperValu II*; *see also In re LinkedIn User Priv. Litig.*, 932 F.Supp. 2d 1089, 1093-94 (N.D. Cal. 2013). Here, Plaintiffs' theory is even more untenable because they do not allege having paid Defendants for *any* goods or services—nor could they. *See Burger v. Healthcare Mgmt. Sols.,* No. 23-1215, *LLC*, 2024 WL 473735, at *6 (D. Md. Feb. 7, 2024) (dismissal for lack of standing where plaintiff did not allege they paid anything); *see also Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1089 (E.D. Cal. 2015) (rejecting benefit of the bargain theory where plaintiff failed to "allege[] that the value of his health care coverage after the Data Breach is less than what it was before the Data Breach").

Diminution in Value Theory. Likewise, "courts have rejected allegations that the diminution in value of personal information can support standing." *In re: Samsung*, 2025 WL 271059, at *11 (dismissal because alleged lost value of PII does not confer standing). Plaintiffs assert that data "is valuable property," CAC ¶ 296, but "have not alleged that they have attempted to sell their personal information or that, if they have, the [Cyberattack] forced them to accept a decreased price for that information." *Chambliss v. Carefirst Inc.*, 189 F. Supp. 3d 564, 572 (D. Md. 2016). Moreover, Plaintiffs do not plausibly allege how their data lost value at all. Their "lost value" theory is an unsupported legal conclusion that "is therefore entitled to no assumption of truth" and cannot support a claim. *Fraga v. UKG Inc.*, No. 22-20105-CIV, 2022 WL 19486310, at *10-13 (S.D. Fla. May 10, 2022) (collecting cases and rejecting "lost value" theory in data breach case); *see also Hubbard*

v. Google LLC, No. 19-cv-07016, 2024 WL 3302066, at *9-10 (N.D. Cal. 2024) (collecting cases and dismissing claims where sole alleged injury was "lost value" of personal data).

Emotional Harms. The No Injury Plaintiffs do not allege any emotional harm.[7] To the extent Plaintiffs collectively allege categorical harms including emotional distress, *see, e.g.*, CAC ¶ 15, anxiety and other intangible harms "fall short of cognizable injury" *Ojogwu v. Rodenburg L. Firm*, 26 F.4th 457, 463 (8th Cir. 2022) (citing *Buccholz v. Meyer Njus Tanick, PA*, 946 F.3d 855, 864 (6th Cir. 2020) (holding "undue sense of anxiety" is not a concrete harm that can confer Article III standing); *Pennell v. Glob. Tr. Mgmt, LLC*, 990 F.3d 1041, 1045 (7th Cir. 2021) (holding that "stress by itself with no physical manifestations and no qualified medical diagnosis" does not amount to a concrete harm).

Spam Calls and Related Nuisances. If Plaintiffs allege injury from nuisances such as receiving increased spam calls, texts, or emails, courts have routinely rejected these purported harms as a basis for standing. *See, e.g.*, *Williams v. Bienville Orthopaedic Specialists, LLC*, 737 F. Supp. 3d 411, 421 (D. Miss. 2024) (dismissing plaintiff for lack of standing based on increase in spam calls even when a caller had plaintiff's name, date of birth, and Medicare number). As one court recently explained: "[s]pam calls are annoying. But an annoyance isn't an actual and concrete injury." *Jenkins*, 2025 WL 78574, at *6.

B. No Plaintiff Can Plausibly Allege Any Injury Is Traceable to the Cyberattack

Plaintiffs attribute every post-February 2024 malady to the Cyberattack despite their acknowledgement that breaches—including hundreds of healthcare breaches—impact tens

[7] *See* CAC ¶¶ 43-44, 66-67, 84-87, 126-27, 132-37.

of millions of Americans annually. CAC ¶¶ 335-36. On close inspection, the CAC is riddled with contradictions and "fails to explain how the PII disclosed in the data breach connects to the injury alleged." *Jenkins*, 2025 WL 708574, at *7. This mismatched pleading—*i.e.*, the harms alleged could not be caused by the data impacted in or timing of this attack—means Plaintiffs failed to establish Article III traceability and must be dismissed.

First, certain of Plaintiffs' alleged injuries *predate* the Cyberattack or alleged availability of data stolen from Change. Plaintiffs allege that ransomware was deployed on February 21, 2024, and that a ransom was paid within one week. CAC ¶¶ 10, 11, 276. For example, Plaintiff Loforese states that his "Personal Information was on the dark web on January 8, 2024," over a month *before* the Cyberattack, highlighting that any harm to Loforese *must* have resulted from a different source of information. *Id.* ¶ 92. Other Plaintiffs do not provide a time period for their alleged injuries—despite having the knowledge to do so—and thus fail to plead that they were harmed after the Cyberattack.

Second, alleged harms post-dating the ransom payment are likewise insufficient. *See Patterson v. Med. Rev. Inst. of Am., LLC*, No. 22-cv-00413, 2022 WL 2267673, at *3 (N.D. Cal. June 23, 2022) (holding undisputed evidence of ransom payment in data breach case supported dismissal for lack of injury); *Practicefirst*, 2022 WL 354544, at *5 (noting that evidence of ransom payment supported conclusion that data had not been used for identity fraud and supported dismissal for lack of injury).

Third, certain Plaintiffs allege unauthorized activity on accounts that Plaintiffs opened *after* the Cyberattack. For example, Plaintiff Phillips alleges that she replaced her credit cards sometime between the Cyberattack and July 2024. CAC ¶ 21. After replacing

her cards, she continued to "learn of fraudulent charges." *Id.* Any new card numbers could not have been impacted by the Cyberattack and therefore these injuries cannot be fairly traced to Defendants. *See also id.* ¶ 108 (alleging unauthorized transactions on a bank account created in September 2024, long *after* the Cyberattack occurred).

Fourth, numerous Plaintiffs allege that they incurred unauthorized charges on their credit cards, debit cards, or bank accounts, but do not allege that Change held information regarding those cards or accounts, or that such information was exfiltrated or made available via the dark web. *See generally id*. It is unsurprising that no Plaintiff alleges that they provided their credit, debit, banking, or other financial information to Change (or any Defendant), because Change is largely a behind-the-scenes participant in the healthcare ecosystem. *See id.* ¶¶ 163; 187. It is not plausible, therefore, that a bad actor could use a Plaintiffs' name, address, date of birth, health insurance group number, and even SSN, to charge an *existing* card or bank account. *See Jenkins*, 2025 WL 708574, at *7 (dismissing claim of unauthorized charges for failure to "plead[] allegations that, if true, trace how unauthorized actors could use the disclosed PII (his name, Social Security number, and date of birth) to make unauthorized PayPal purchases or steal his money").

Fifth, numerous other injuries complained of could not have reasonably transpired by using data held by Change that was allegedly impacted. Plaintiffs allege that they received Notice of Data Breach letters from Change, which advised that the "data that may have been seen and taken" includes contact information and one or more types of additional information, including health insurance member/group ID numbers, and was not the same for everyone. *See, e.g.*, Ex. 1, Notice Letter, *Coletti, et al. v. Change Healthcare, Inc.*, No.

0:24-cv-03681, ECF No. 1-1 (D. Minn. Sept. 17, 2024);[8] *see also* CAC ¶ 178 (describing data allegedly held by Change). Even if this information was made available on the dark web (it was not), it is not plausible that someone could use that information to, for example, attempt to access Plaintiff Christenson's iCloud or CashApp accounts, *id.* ¶ 17, Plaintiff Abramazyk's online Walmart account, *id.* ¶ 106, Plaintiff Tynch's Amazon account, *id.* ¶ 122, or Plaintiff Anderson's Sirius XM radio account, *id.*, ¶ 144.

Lastly, Plaintiffs allege as injuries outreach that they received from unknown sources regarding people, accounts, products, and services that they do not recognize, and that are entirely unrelated to the Cyberattack and Defendants. *See, e.g.*, CAC ¶ 94 (alleging Plaintiffs' information was found online in relation to a clinical trial she did not participate in); ¶ 144 (alleging Plaintiff received a letter in the mail regarding a Mercedes he does not own); ¶ 17 (alleging receipt of emails to individual who is unknown to her); ¶ 49 (alleging attempt to access non-existent Credit Karma account); ¶ 96 (alleging receipt of communications regarding non-existent Amazon account). Plaintiffs fail to allege how these are injuries at all, let alone harms caused by any Defendant's conduct. Indeed, they suggest that Plaintiffs' PII is available via sources *other* than as a result of the Cyberattack. As such, these harms should be dismissed for lack of traceability.

[8] Each Plaintiff alleges receipt of a Notice letter, but do not attach their letters as exhibits. *See generally* CAC ¶¶ 17-147. Plaintiffs in other cases in this MDL attached their letters, including Mr. Coletti. Like Plaintiffs Mammad and Harbon's letters, Mr. Coletti's letter was dated July 29, 2024. *See id.* ¶ 29 (alleging receipt of a notice letter dated July 29, 2024); ¶ 114 (same). The Court may consider the notice letter in *Coletti* without converting this motion to dismiss into a motion for summary judgment. *See, e.g.*, *Zean*, 858 F.3d at 526.

II. INJURIES THAT CANNOT SUPPORT ARTICLE III STANDING SHOULD BE STRUCK & THE CLASS DEFINITONS NARROWED

The Court can and should strike the categories of injury that cannot—on their own—confer standing. Specifically, Rule 23(d)(1)(D) permits the Court to direct the amendment of the pleadings "to eliminate allegations about representation of absent persons." As such, the Court should amend the proposed class definitions to exclude injuries that cannot confer standing by appending the following to each:

> *except individuals that experienced only: a loss of privacy, misappropriation of their identity, diminution of the value of their Personal Information, lost value of their Personal Information, emotional and mental distress, receipt of spam or phishing calls, texts, or emails, and/or lost time, effort, and/or expense attempting to mitigate the impact of the Cyberattack.*

If these injuries are not excluded, Plaintiffs' putative classes run afoul of the Eighth Circuit and Supreme Court's requirement that "each member [of a class] must have standing and *show an injury in fact* that is traceable to the defendant." *Halvorson,* 718 F.3d at 778. "Permitting such allegations to remain [prejudices] the defendant by requiring the mounting of a defense against claims that ultimately cannot be sustained." *Donelson v. Ameriprise Fin. Servs. Inc.*, 999 F.3d 1080, 1092 (8th Cir. 2021) (internal quotation omitted). If Plaintiffs are able to establish standing based on certain injuries, now or at any time in the future, they should not be allowed to later bring "unsupportable class allegations" based on other injuries that cannot confer standing. *Id.*

This is not an abstract concern. It has become common practice in data breach class actions to rely on allegations of fraud to establish standing at the outset of a case, only to abandon those theories of liability at class certification in favor of injuries that limped by

the motion to dismiss by piggybacking on the "actual" harms. Indeed, Defendants are aware of no data breach class certification motion where Plaintiffs relied on actual fraud to support class certification. *See, e.g.*, *In re Blackbaud, Inc. Customer Data Breach Litig.,* No. 3:20-mn-02972,2024 WL 2155221, at *26 n.41 (D.S.C. May 14, 2024) (proposed class-wide damages model based on purported lost value of data and the cost of mitigation products); *In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig.*, 341 F.R.D. 128, 153-54 (D. Md. 2022) (proposed class-wide damages model based on "overpayment" for hotel rooms as a result of data breach and "loss of market value of PII").

Courts faced with the prospect of overbroad class definitions have struck class allegations entirely from the complaint. For example, in *Edwards v. Zenimax Media Inc.*, a plaintiff brought a claim against a video game manufacturer alleging injury from a technical error that prevented him from completing the game. No. 12-cv-00411, 2012 WL 4378219, at *1 (D. Colo. Sept. 25, 2012). The proposed class, however, consisted of every purchaser of the game in that state. *Id.* at *5. The *Edwards* court determined that the class definition included individuals that were not possibly injured and struck the class allegations from the complaint under Rule 23(d)(1)(D) prior to the start of discovery.[9] *Id.* at *6-7; *see also Lyons v. Bank of Am., NA*, No. C 11-1232, 2011 WL 6303390, at *7 (N.D.

[9] The Court may also strike these allegations under Rule 12(f). *See Gilbert v. United States Olympic Comm.*, No. 18-cv-00981, 2019 WL 1058194, at *32-33 (D. Colo. Mar. 6, 2019) (*R. & R. adopted in relevant part* 423 F. Supp.3d 1112, 1155 (D. Colo. 2019) (striking class allegations under Rule 12(f), as "redundant, immaterial, impertinent, or scandalous" and explaining that there is no practical distinction between a motion to strike class action allegations under Rules 12(f) or 23(d)(1)(D)).

Cal. Dec. 16, 2011) (granting early motion to strike "[b]ecause the proposed class includes many members who have not been injured"); *Sanders v. Apple Inc.*, 672 F. Supp.2d 978, 990-91 (N.D. Cal. 2009) (granting early motion to strike because class definition included uninjured parties and noting "[t]he class must therefore be defined in such a way that anyone within it would have standing"); *Tietsworth v. Sears*, 720 F.Supp.2d 1123, 1146-47 (N.D. Cal. Mar. 31, 2010) (granting early motion to strike "because the purported class includes members who have suffered no injury"); *Hovsepian v. Apple, Inc.*, No. 08-5788 (PVT), 2009 WL 5069144, at *6 (N.D. Cal. Dec. 17, 2009) (striking class allegations because any eventual class would include individuals who suffered no Article III injury).

Here, Defendants do not seek the "extreme" step of striking all class allegations on the pleadings. *Donelson*, 999 F.3d at 1092 (internal quotation omitted). Rather, this Motion aims to weed out the categories of injuries that cannot confer standing and are therefore irrelevant to any subsequent litigation. This action is appropriate now because "it is apparent from the pleadings" that the identified injuries cannot confer standing as a matter of law and no discovery could change that determination. *See id.* (holding district court erred by denying Motion to Strike class allegations at the pleadings stage where deficiencies were apparent). By paring down the pleadings now, fact and expert discovery can more efficiently focus on injuries that can confer Article III standing, and related damages theories, in line with Eighth Circuit and Supreme Court requirements.

III. PLAINTIFFS CANNOT ADEQUATELY PLEAD CAUSATION AND INJURY TO MEET RULE 12(B)(6)'S REQUIREMENTS

Even if Plaintiffs clear Article III, they have not met the higher requirement to plead the causation and injury elements of their claims. *See, e.g.*, *SuperValu II,* 870 F.3d at 773; *Brown v. Medtronic, Inc.*, 628 F.3d 451, 459 (8th Cir. 2010). Indeed, Plaintiffs' claims should be dismissed because they failed to allege the higher standard of cognizable injury under Rule 12(b)(6), any action or inaction by Change or the Non-Change Defendants proximately caused their injuries, or both. Courts in many data breach cases reached this conclusion on substantially similar facts, and this Court should do the same.

A. Alleged Fraud Without Monetary Loss Fails to State a Cognizable Injury

Plaintiffs must "plead facts sufficient to raise a right to relief above the speculative level" in order to clear the "higher hurdles" of Rules 8(a) and 12(b)(6). *In re: SuperValu, Inc., Customer Data Sec. Breach Litig.*, No. 14-MD-2586, 2018 WL 1189327, at *10 (D. Minn. Mar. 7, 2018) ("*SuperValu III*"). They have failed to do so.

The Eighth Circuit has held that a plaintiff must affirmatively plead out-of-pocket loss, rather than merely rely on an inference of loss, to survive a motion to dismiss. *SuperValu IV*, 925 F.3d at 965 (upholding dismissal where plaintiff failed to allege out-of-pocket losses from fraudulent charges). Plaintiffs are "in the best position to know whether [they were] ever obligated to pay [an] unauthorized charge," and the Court is "not required to draw unreasonable inferences in [their] favor." *Id.* Plaintiffs fail to allege the injury under every claim to the extent they allege (1) an unauthorized transaction without alleging

having incurred out-of-pocket losses due to unreimbursed charges, (2) an "attempted" phishing attempt or transaction, or (3) merely normal, consumer-related communications.

"[A] cardholder's mere allegation of an unauthorized charge, unaccompanied by an out-of-pocket loss, is not sufficient to state an actionable injury." *SuperValu III*, 2018 WL 1189327, at *11. Likewise, "unauthorized withdrawals and bank fees" are not a cognizable injury if they are reimbursed. *In re: Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 527 (N.D. Ill. 2011). Here, numerous Plaintiffs allege unauthorized financial transactions, but the case law is clear that those fail where Plaintiffs allege no unreimbursed, out-of-pocket costs. *SuperValu III,* 2018 WL 1189327, at *10. Nearly all Plaintiffs who allege an unauthorized charge do not specify the amounts and do not allege that those amounts went unreimbursed by the bank, or were paid by Plaintiffs.[10] For example, Plaintiff Jones claims she "learned of an unauthorized charge on her Bank of America account" but does not allege the amount of the charge or that she actually had to pay the charge. CAC ¶ 80. In fact, several Plaintiffs who allege "out-of-pocket costs" are in fact alleging mitigation expenses, not losses caused by fraudulent transactions.[11] *Id*. For example, Plaintiff Kleinheksel alleges "$6 in out-of-pocket costs…by purchasing an identity tracker" but no unreimbursed fraud. *Id.* ¶ 56.

[10] *See, e.g.*, CAC ¶ 58 (alleging an eye doctor charged her VSP Vision Account, but not the amount charged or that she paid it); *id.* ¶ 92 (alleging unauthorized charges and their amounts, but not that he paid them); *id.* ¶ 104 (alleging unauthorized charge and the amount, but not that she paid it).

[11] *See, e.g.*, CAC ¶ 106 (alleging fraudulent charges but that Plaintiffs' purported "out-of-pocket costs" are from purchasing credit monitoring services).

Similarly, numerous Plaintiffs allege activity that they frame as indicative of *attempted* fraud, but the Court should hold—"draw[ing] on its judicial experience and common sense"—that these attempts do not constitute fraud (let alone monetary loss).[12] *Hamilton v. Palm*, 621 F.3d 816, 818 (8th Cir. 2010) (internal quotations omitted). Plaintiff Evans, for example, alleges an "unauthorized *attempt* to withdraw" money from her account but does not allege she lost any money. CAC ¶ 70.

Finally, numerous Plaintiffs allege activity that they frame as indicative of attempted phishing or misuse of PII, but these activities do not constitute (or even suggest) fraud. Instead, these allegations amount to legitimate activities—like online shopping, holding debit and credit card accounts, home ownership, and other everyday activities unrelated to the Cyberattack or any of the Defendants.[13] For example, Plaintiff Korlou alleges that recruiting emails for a marketing analyst position are indicative of fraud when he has worked in the marketing field for two decades. *Id.* ¶ 98.

B. Allegations that Plaintiffs' PII Appeared on the Dark Web Are Insufficient

Many Plaintiffs allege their data is available on the dark web but do not state when they were notified that their data was on the dark web, what data elements were available, whether Change held that information about them, or when the data was actually posted.

[12] *See, e.g.*, CAC ¶ 17 (alleging *attempted* unauthorized charges); *id.* ¶ 44 (alleging *attempted* fraudulent charge); *id.* ¶ 140 (alleging someone *tried* to access account); *id.* ¶ 100 (alleging *attempted* access to account); *id.* ¶ 102 (alleging *attempted* withdrawal).

[13] *See, e.g.*, CAC ¶ 17 (applied for a loan that was denied); *id.* ¶ 33 (received emails from a law group); *id.* ¶ 88 (received "junk emails" mentioning unknown people); *id.* ¶ 94 (received calls "attempting to sell 'mystical' products"); *id.* ¶ 96 (received text regarding nonexistent account); *id.* ¶ 104 (received calls regarding vehicle coverage).

Allegations that a plaintiff's information was available on the dark web, without any further allegation of financial misuse or harm, is ***not*** sufficient to survive a motion to dismiss. *Bonewit v. New-Indy Containerboard LLC*, No. 24-cv-11338, 2024 WL 4932186, at *4 (D. Mass. Dec. 2, 2024) (dismissing claim for lack of compensable injury because plaintiff failed to allege any further harm beyond their data being posted on the dark web). Plaintiffs Avery, Dugan, Madonna, Warren, Sims, Powers, Brooks, Hoag, Lanier, Harbon, Rush, and Ivory thus have failed to state any injury sufficient to survive this Motion.[14] These Plaintiffs, and Counts XIV, XVIII, XXXIII, XXXVI, and XXXIX, must be dismissed.

C. Plaintiffs Cannot Satisfy the Heightened Causation Requirements of 12(b)(6)

Even if the Court accepts that a particular alleged injury is "fairly traceable" to the Cyberattack for standing, each individual Plaintiff has failed to sufficiently allege that such injuries were proximately caused by any Defendant. *SuperValu III*, 2018 WL 1189327, at *10-11 (noting that "proximate cause" on a motion to dismiss presents "higher hurdles" than Article III's "fairly traceable" requirement). In *SuperValu III*, the Court held that allegations that "establish only the sheer possibility that [an alleged fraudulent] charge was attributable to the data breach" were insufficient to state a claim for relief. *Id* at *13. As another example, under Tennessee law, "[p]roof of causation equating to a 'possibility,' a

[14] CAC ¶ 23 (alleging PI appeared on the dark web, but not when or that any misuse transpired); ¶ 27 (same); *id.* ¶ 31 (same); *id.* ¶ 33 (same); *id.* ¶ 112 (same); *id.* ¶ 138 (same); *id.* ¶ 47 (alleging PI appeared on the dark web post-Cyberattack, but not that any misuse transpired); *id.* ¶ 54 (same); *id.* ¶ 72 (same); *id.* ¶ 74 (same); *id.* ¶ 124 (same); *id.* ¶ 114 (same, and separately, that Plaintiff engaged in a "fake job interview"); *id.* ¶ 82 (alleging PI appeared on the dark web, but not that any misuse transpired; and that Plaintiff elected to incur a cost).

'might have,' 'may have,' or 'could have,' is not sufficient, as a matter of law, to establish the required nexus between the plaintiff's injury and the defendant's tortious conduct." *Robbins v. Perry Cnty.*, No. M2008-00548-COA-R3-CV, 2009 WL 1162579, at *4 (Ct. App. Tenn. 2009) (alterations in original) (*quoting Kilpatrick v. Bryant*, 868 S.W.2d 594, 602 (Tenn. 1993)). Because Plaintiffs cannot meet this heightened causation standard, their claims must be dismissed. *See supra* Section I.B. (describing causation failures in CAC).

IV. PLAINTIFFS FAIL TO STATE A CLAIM AGAINST THE NON-CHANGE DEFENDANTS THAT DID NOT SUFFER THE CYBERATTACK

Change was the victim of the Cyberattack and is the focus of Plaintiffs' Complaint. Yet, Plaintiffs attempt to assert claims against UHG, Optum, Inc., and OptumInsight, Inc. (the "Non-Change Defendants") by suggesting that because UHG acquired Change and the Non-Change Defendants provided support to Change *post*-Cyberattack, they must have owed duties to Plaintiffs to protect PII or may be held liable for purported deficiencies in Change's cybersecurity *pre*-Cyberattack.[15] Not so.

"A parent corporation . . . is not liable for the acts of its subsidiaries." *United States v. Bestfoods*, 524 U.S. 51, 61 (1998). Plaintiffs ignore that each entity under UHG operates as a separate legal entity, with its own responsibilities and obligations under the law. *See Manigault-Johnson v. Google, LLC*, No. 2:18-cv-1032, 2019 WL 3006646 (D.S.C. Mar. 31, 2019) (dismissing parent company in privacy action because Plaintiffs failed to allege

[15] *See, e.g.*, CAC ¶ 407 (suggesting the Non-Change Defendants owed a duty to secure Plaintiffs' PII because UHG helped investigate and respond to the Cyberattack); *id.* ¶ 262 ("Following the data breach, UHG continued to issue a series of notifications . . . ."); *id.* ¶ 277 (UHG's CEO "made the decision to pay the ransom").

"any independent wrongdoing on the part of" parent). Ordinary actions such as "monitoring of the subsidiary's performance, supervision of the subsidiary's finance and capital budget decisions, and articulation of general policies and procedures, should not give rise to direct liability." *Bestfoods*, 524 U.S. at 72 (internal quotation omitted).

It is also well-understood that "[p]leadings setting forth the collective actions of the 'defendants' fail to make out a prima facie . . . case for individual liability against any defendant who is not alleged to have taken part in other specific acts." *Smith v. AVSC Int'l, Inc.*, 148 F. Supp. 2d 302, 312 (S.D.N.Y. 2001). Plaintiffs improperly group "all Defendants" together without clarifying the role of each in the alleged conduct, group Defendants but call out Change in the same breath, or broadly assert UHG "controlled" or "oversaw" Change cybersecurity.[16] *See Dorosh v. Minn. Dep't of Hum. Servs.*, No. 23-cv-1144 (ECT/LIB), 2023 WL 6279374, at *6 (D. Minn. Sept. 26, 2023) (dismissing claims for not satisfying Rule 8(a) where defendants were "lumped" together).

V. PLAINTIFFS' NEGLIGENCE CLAIM FAILS BECAUSE THERE IS NO DUTY, MUCH LESS BREACH OR RESULTING HARM

Plaintiffs' negligence claim fails under the laws of every state because Plaintiffs fail to allege any duty owed by Change or by the Non-Change Defendants.[17] Also, to the extent

[16] *See, e.g.*, CAC ¶ 398 ("Defendants operated as a single unit"); *id.* ¶ 2 ("Defendants, and, in particular, Change Healthcare"); *id.* ¶ 407.

[17] This Memorandum of Law incorporates the choice-of-law arguments submitted in a standalone brief filed concurrently herewith. As detailed in that brief, Minnesota choice-of-law rules apply to Plaintiffs' claims, and under Minnesota law, (i) each Plaintiff's tort claims are governed by the laws of their home states, (ii) each Plaintiff's breach of contract claims are governed by any choice-of-law provision in the contract itself, but (iii) in the absence of a choice-of-law provision in a Plaintiff's contract, the contract claim is governed

certain Plaintiffs seek to redress purported harms stemming from pharmacy services downtime without pleading a duty to provide uninterrupted pharmacy services, their negligence claim likewise fails for lack of duty. Moreover, Plaintiffs have not sufficiently alleged a breach of *any* duty owed. Finally, Plaintiffs' alleged damages are purely economic and barred by the economic loss rule in several states.

A. There Is No Common Law Duty to Safeguard Information or to Notify

Plaintiffs allege that Defendants owed them "a duty to exercise reasonable care in securing" their data. CAC ¶ 401. However, courts in data breach cases routinely hold that no common law duty to safeguard personal information exists.[18] *See, e.g.*, *SuperValu IV*, 925 F.3d at 962-63 (finding no duty to safeguard sensitive personal or financial information under Illinois law); *see also* Appendix A.[19] There is no reason for this federal Court to depart from this settled state precedent here.

Recognizing there is no general duty to safeguard information, Plaintiffs claim a duty arises from the "sensitive nature" of the data and a "foreseeable" injury. CAC ¶ 401. Plaintiffs generally and broadly allege that "sensitive" information is "stored" by Change

---

by Plaintiff's home state. However, even if the Court finds that Minnesota substantive law applies to Plaintiffs' claims.

[18] As described *supra* Section II.D, Plaintiffs have failed to state any duty owed by a Non-Change Defendant to protect PII held *by Change* on behalf of *Change* customers.

[19] *See also Aspen Am. Ins. Co. v. Blackbaud, Inc.*, No. 3:22-CV-44, 2023 WL 3737050, at *4-5 (N.D. Ind. May 31, 2023) (finding "no common law duty to safeguard the public from the risk of data exposure" under Indiana law and dismissing negligence claim); *Gorman v. Ethos Grp. Inc.*, No. 3:22-cv-02573-M, 2024 WL 1257493, at *3 (N.D. Tex. Mar. 25, 2024) (declining to create duty under Texas law); *Smahaj v. Retrieval-Masters Creditors Bureau, Inc.*, 131 N.Y.S.3d 817, 825 (N.Y. Sup. Ct. 2020) ("no duty to protect plaintiff from third parties harming her"); *Dep't of Labor v. McConnell*, 828 S.E.2d 352, 358 (Ga. 2019) (same); *Pirozzi v. Apple, Inc.*, 913 F. Supp. 2d 840, 851-52 (N.D. Cal. 2012) (same).

(or "Defendants"), and thus suggest it must have been impacted by the Cyberattack. *Id.* ¶¶ 166, 403. But Plaintiffs *do not* allege that any sensitive information about them was exposed, and the Court should not make that leap. *See, e.g.*, *id.* ¶ 405 (alleging merely that Defendants "collected and stored highly sensitive information"); *id.* ¶ 412 (alleging cybercriminals "accessed" putative class members' personal information). Even if we ignore this failure, courts have dismissed negligence claims predicated on a duty to safeguard health data. *See Attias v. CareFirst, Inc.,* 365 F. Supp. 3d 1, 24 (D.D.C. 2019) (dismissing negligence claim because "every day interactions with a health insurance provider" did not create duty to safeguard "private information").

Plaintiffs cannot point to HIPAA to save their claim either. HIPAA does not create a common law duty to protect PII. *Haywood v. Novartis Pharms. Corp.*, 298 F. Supp. 3d 1180, 1191 (N.D. Ind. 2018) ("HIPPA [sic] does not create a duty or provide a statutory basis" for plaintiff's claim). And "[c]ourts are leery of imposing a state common law duty based on a federal statute lacking a private right of action," like HIPAA, *Harris v. Nationwide Mut. Fire Ins. Co.*, 367 F. Supp. 3d 768, 776 (M.D. Tenn. 2019), because that would be "tantamount to authorizing a prohibited private right of action," *Sheldon v. Kettering Health Network*, 40 N.E.3d 661, 672 (Ohio Ct. App. 2015).[20]

[20] Count I references a duty based on HIPAA. Elsewhere in the CAC, Plaintiffs allege that Defendants failed to comply with Section 5 of the FTC Act. To the extent Plaintiffs claim this statute creates a duty to safeguard data, that argument also fails. *See, e.g.*, *In re LastPass Data Sec. Incident Litig.*, 742 F. Supp. 3d 109, 124 (D. Mass. 2024) (holding the FTC Act does "not establish a duty cognizable in negligence").

Nor is there a common law duty to "timely and accurately disclose the scope, nature, and occurrence of the Data Breach." CAC ¶ 404. Instead, courts have rejected attempts to create common law notification obligations due to the existence of state data breach notification statutes. *See Cmty. Bank of Trenton v. Schnuck Mkts., Inc.*, No. 15-cv-01125, 2017 WL 1551330, at *2 (S.D. Ill. May 1, 2017) (dismissing negligence claim in part because data breach notification law implied no common law duty to notify); *see also Aspen Am. Ins. Co.*, 2023 WL 3737050, at *4 (lack of private right of action in state statute precludes common law duty to notify); *Malone v. Norwest Fin. Cal. Inc.*, 245 B.R. 389, 396 (E.D. Cal. 2000) ("[T]he existence of statutory remedies militates against implying additional relief.").

This Court should adopt "the narrower and more reasonable path" and reject the invitation to create a new state law duty. *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 636 (7th Cir. 2007) (internal quotation omitted). It is a "well-established principle that where two competing yet sensible interpretations of state law exist, [federal courts] should opt for the interpretation that restricts liability, rather than expands it." *Travelers Indem. Co. v. Dammann & Co.*, 594 F.3d 238, 253 (3d Cir. 2010) (internal quotations omitted).

B. There Is No Duty to Provide Uninterrupted Services

Eight Plaintiffs allege that they were injured due to the disruption of medical care or pharmacy services when Change immediately took services offline to prevent the threat actor from accessing other systems. CAC ¶¶ 25, 37, 39, 56, 76, 110, 116, 128. Yet Plaintiffs have not even pled that Defendants owed them a separate, cognizable duty to provide uninterrupted services. *See id.* ¶¶ 327, 328, 391, 401-05, 408-09, 417, 455, 561, 568, 735

(alleging Defendants owed a duty to safeguard "Personal Information" but not to provide uninterrupted services). This is not surprising, because, as confirmed by *Colonial Pipeline*, there is no common law or statutory duty to provide continuous business-to-business services, *see* Provider Track Motion to Dismiss, Section II.B.i, let alone a duty to ensure that these services are available *to Plaintiffs*, who have no contractual relationship with Change. *See Dickerson v. Colonial Pipeline Co.*, No. 1:21-CV-2098, 2022 WL 18717801 (N.D. Ga. June 17, 2022).

Specifically, in *Colonial Pipeline*, the defendant operated a pipeline that supplied "nearly half" of the fuel consumed across the East Coast. *Id.* at *1. The defendant shut down the pipeline while recovering from a cyberattack, which "decreased the supply of gasoline . . . and caused the price of gasoline to rise." *Id.* The plaintiffs were individual consumers who alleged that the cyberattack caused them to pay more for gasoline than they otherwise would have had defendants' services remained uninterrupted. *Id.* at *2. Plaintiffs alleged a duty "to continually provide services" and a "duty to safeguard information." *Id.* at *2. The court dismissed their negligence claim because, *inter alia*, plaintiffs failed to allege that defendants owed them "any cognizable statutory or common law duty" to provide uninterrupted services. *Id.* at *3. The court also rejected plaintiffs' argument that the harm could be based on a duty to safeguard PII from disclosure because, even assuming that such a duty existed,[21] that duty (to safeguard PII) was too divorced from the alleged

[21] The Court cast doubt on whether such a duty existed, noting that "the Eleventh Circuit has questioned the existence under Georgia law of an independent common law duty to safeguard and protect . . . personal information." *Colonial Pipeline*, 2022 WL 18717801,

harm (paying more for gas while defendants' services were unavailable). *See Colonial Pipeline*, 2022 WL 18717801, at *5 (disclosure of PII "is not the alleged injury that occurred in this case").

The facts here are similar. Plaintiffs allege that Defendants owed them a duty to use reasonable care to safeguard their PII from disclosure. *See* CAC ¶¶ 327, 328, 391, 401-405, 408-409, 417, 455, 561, 568, 735. But they allege harms purportedly related to (1) the potential disclosure of their PII; and (2) Change's services disruption (e.g., delay in filling a prescription). *See, e.g.*, *id.* ¶¶ 15, 56 ("Plaintiff Kleinheksel's prescription medication was delayed twice in or about February 2024.").[22] Like in *Colonial Pipeline*, Plaintiffs' failure to allege that Change or any Non-Change Defendant owed them a duty for Change to provide uninterrupted services to Plaintiffs—and the clear lack of any such duty—is fatal to their negligence claim based on purported pharmacy-related harms.

C. Plaintiffs Do Not Plausibly Allege Breach

Even if a duty exists—whether to safeguard information or to notify—Plaintiffs fail to allege a breach of either duty. Plaintiffs suggest that because the Cyberattack occurred, Change's remote access, network monitoring, and data segregation practices must have

---

at *5 n.7 (internal quotation omitted) (quoting *Murray v. ILG Techs., LLC*, 798 F. App'x 486, 492 (11th Cir. 2020)).

[22] *See also* CAC ¶¶ 413, 425, 434, 447, 473, 489, 499, 515, 533, 548, 592, 612, 638, 655, 666, 682, 702, 724, 745, 761, 791, 811, 822, 839, 862, 878, 900, 916, 934, 949, 961, 980, 996, 1013, 1028.

been deficient.[23] CAC ¶ 409. Plaintiffs invite the court to adopt a *res ipsa loquitur* approach and assume that because the threat actor committed a cyberattack, Defendants must have been negligent. This is not the law. *See* Order, *Crowe v. Managed Care of N. Am.*, No. 0:23-cv-61065-AHS, ECF No. 160, at 20 n.8 (S.D. Fla. Aug. 16, 2024) ("*MCNA* Order") (dismissing negligence claim for failure to allege a breach of duty to safeguard information, and highlighting that because a "leading international hacker with thousands of cyberattacks to its credit [was] responsible, it is certainly possible that Defendants' data security systems could have been strong and in compliance with Defendants[']statutory obligations").

Indeed, Plaintiffs' allegations show that Defendants acted reasonably and still Change was the victim of a criminal gang, like thousands of other entities. *See* CAC ¶ 270 (explaining UHG thwarts over 450,000 intrusions annually, or "a cyberattack attempted every 70 seconds"); *id.* ¶ 245 (alleging this threat actor victimized over 1,000 companies); *id.* ¶¶ 234, 239, 254 (stating the threat actor was a "sophisticated threat to the health sector" that used a "notably sophisticated" programming language, and that "moved laterally within the systems in more sophisticated ways"). These allegations fail to support a breach of duty. *See, e.g.*, *MCNA* Order at 10-14, 20 (dismissing negligence claim because plaintiffs' allegations "impose[] an unfair responsibility upon companies with the best

[23] It is unclear whether Plaintiffs claim that Defendants breached a duty to monitor Change systems, separate from an allege duty to secure information. To the extent they plead a duty to reasonably monitor network activity, Plaintiffs again fail to provide any evidence of the existence of that duty or breach by Defendants. *See MCNA* Order, at 12 (rejecting the idea that "a security system is inadequate if it fails to detect a breach instantaneously").

intentions" and "requires companies to always be one-step ahead of cybercriminals, otherwise they may face legal liability").

Plaintiffs also fail to state any breach of an alleged duty to timely notify. Every Plaintiff states that they received a notice letter. *See generally* CAC ¶¶ 17-147. And no Plaintiff alleges a date by which they should have received notice sooner. *Id*. Plaintiffs have not pled what a "breach" of this duty would be, much less how it occurred here.

D. The Economic Loss Rule Bars Plaintiffs' Negligence Claims in Many States

Finally, the economic loss rule bars the negligence claims for 21 Plaintiffs under 15 states laws. *See* Appendix A. The rule precludes tort claims in those states that do not allege damage to persons or property. *Arena Holdings Charitable, LLC v. Harman Prof'l, Inc*., 785 F.3d 292, 293 (8th Cir. 2015). This is because economic losses are best allocated through agreements between sellers and purchasers, rather than through the duties associated with torts. *Cmty. Bank of Trenton v. Schnuck Mkts., Inc.*, 887 F.3d 803, 812-16 (7th Cir. 2018). Plaintiffs do not allege physical injury or property damage, and courts routinely dismiss negligence claims in data breach cases where harms are economic.[24] *See, e.g.*, *id.* at 817-19; *see also* Appendix A.

[24] The economic loss rule does not require a direct contractual relationship between the parties; it also applies where plaintiffs allege they are third-party beneficiaries of a contract, as Plaintiffs do here. *Brickman v. Maximus, Inc.*, No. 2:21-cv-3822, 2023 WL 2563661, at *2 (S.D. Ohio Mar. 17, 2023) (finding economic loss rule applied where plaintiff asserted third-party beneficiary claim).

VI. NEGLIGENCE *PER SE* SHOULD BE DISMISSED BECAUSE IT IS NOT A RECOGNIZED CAUSE OF ACTION, IS BARRED BY THE ECONOMIC LOSS RULE, AND CANNOT RELY ON PURPORTED HIPAA OR FTC ACT VIOLATIONS

Plaintiffs' negligence *per se* claim, predicated on alleged violations of the FTC Act and HIPAA (collectively, "the Federal Statutes"), should be dismissed for several reasons.

First, 16 states do not recognize negligence *per se* at all. *See* Appendix B.

Second, the economic loss rule bars Plaintiffs' claim in 15 states. *See supra* Section V.D; Appendix B.

Third, an alleged violation of the Federal Statutes cannot form the basis of a negligence *per se* claim for additional reasons. Under the law of 24 states, the claim cannot rely on a statute that has no private right of action. *See* Appendix B. Neither of the Federal Statues has a private right of action. *See Guthrie v. Bank of Am., Nat'l Ass'n*, No. CIV. 12-2472, 2012 WL 6552763, at *5 (D. Minn. Dec. 14, 2012) ("[T]he FTCA does not create a private right of action[.]"); *Trone Health Servs., Inc. v. Express Scripts Holding Co.*, 974 F.3d 845, 851 (8th Cir. 2020) ("HIPAA does not create a private right of action as an underlying basis for a civil suit.") (internal quotation omitted). Under the law of Kentucky and Texas, the claim can only rely on penal statutes. Appendix B. Here, Section 5 of the FTC Act is not a penal statute. HIPAA is largely enforced through civil penalties, and Plaintiffs do not allege any facts suggesting a criminal violation.[25] Finally, in 11 states, the statute relied upon must protect a particular "class of persons," not the general public.[26] *Id.*

[25] 42 U.S.C. § 1320d-6(a) (criminal violation requires knowing disclosure of protected health information to unauthorized parties).

The Federal Statutes were enacted to protect the public generally and thus cannot form the basis of Plaintiffs' negligence *per se* claim. *See, e.g.*, *Langbehn v. Pub. Health Tr. of Miami-Dade Cnty.*, 661 F. Supp. 2d 1326, 1342 (S.D. Fla. 2009) (dismissing negligence *per se* claim); *see also* Appendix B.

VII. PLAINTIFFS' BREACH OF CONTRACT CLAIM MUST BE DISMISSED BECAUSE THEY HAVE NOT SPECIFIED CONTRACTS, THE PRESUMPTION AGAINST THIRD-PARTY BENEFICIARIES PREVAILS, AND HIPAA CANNOT FORM THE BASIS OF THEIR CLAIM

In addition to Plaintiffs' failure to allege causation and harm, *see supra* Sections I, III, Plaintiffs' breach of contract claim must be dismissed for at least three other reasons. This claim is premised on alleged Business Associate Agreements ("BAAs") between Defendants and covered entities to which Plaintiffs are not parties. CAC ¶ 431. Generally, "one who is not a party to a contract has no rights under the contract." *Caldas v. Affordable Granite & Stone, Inc.*, 820 N.W.2d 826, 832 (Minn. 2012). The Court thus starts with a presumption that Plaintiffs have no rights to enforce any BAA. *Bricks, Inc. v. BNY Tr. Co. of Missouri*, 165 F. Supp. 2d 723, 726 (W.D. Tenn. 2001). To overcome this presumption, Plaintiffs must plausibly allege (1) the existence of a valid contract; (2) that the parties to the contract clearly intended the contract for Plaintiffs' benefit; and (3) breach. *Id.* Like all contract claims, the contract's plain language controls and "[a]ll doubts must be resolved against conferring third-party beneficiary status." *Bruno v. Donohoe as Tr. of Texas Med. Liab. Tr.*, No. 1:23-CV-01183, 2024 WL 5305079, at *8 (W.D. Tex. Oct. 25, 2024) (internal quotation omitted).

***First*, Plaintiffs fail to plausibly plead the existence of a valid contract.** *Id.*; *see also* Appendix C. To plausibly allege the existence of a valid contract, a plaintiff must allege "offer, acceptance, and bargained for consideration" along with a "meeting of the minds concerning [these] essential elements." *Elsherif v. Mayo Clinic*, No. 18-2998 (DWF/KMM), 2019 WL 1505960, at *2 (D. Minn. Apr. 5, 2019) (quoting *Topchian v. JPMorgan Chase Bank, N.A.*, 760 F.3d 843, 850 (8th Cir. 2014); *Minneapolis Cablesystems v. City of Minneapolis*, 299 N.W.2d 121, 122 (Minn. 1980)). It is axiomatic that to allege a valid contract exists, the Court must know the contracting parties. *E.g.*, *Olsen v. Johnston*, 301 P.3d 791, 794 (Mont. 2013) ("To form a legally enforceable contract, there must be . . . identifiable parties capable of contracting.").

Plaintiffs fail to identify *any* specific parties that allegedly contracted to their benefit. To start, Plaintiffs fail to meet the basic principles of notice pleading required by Rule 8(a) by omitting basic information such as the alleged contracting parties. CAC ¶ 431. Plaintiffs have compounded this problem by asking the Court to assume that (1) Defendants generally "must have" entered into BAAs with unnamed "covered entities"; (2) those BAAs must have included clauses requiring "Defendants" to comply with HIPAA; and (3) a requirement to comply with HIPAA was necessarily "intended to protect patients *like* Plaintiffs[] and the [putative] Class." *Id.* ¶ 432 (emphasis added).[27]

[27] If Plaintiffs had identified specific contracts they believe benefitted them, their claim would likely further deteriorate. Many contracts, including BAAs, expressly disavow the existence of third-party beneficiaries. The presumption against third-party beneficiaries becomes conclusive when "a contract provision expressly stat[es] that nothing within the contract should be construed as creating any third-party beneficiaries." *Partin v. Baptist*

Because Plaintiffs have not identified any contracts or contracting parties at all, they have failed to allege the existence of valid contracts, and their claim for breach of contract as third-party beneficiaries must be dismissed. *See, e.g.*, *Owens v. Rodale, Inc.*, No. 14-12688, 2015 WL 575004, at *4 (E.D. Mich. Feb. 11, 2015) (dismissing claim when plaintiff failed to identify any specific contract at issue and only alleged generally that her subscription agreement incorporated requirements of the Video Rental Privacy Act); *see also Kuchenmeister v. HealthPort Techs., LLC*, 753 F. App'x 794, 797 (11th Cir. 2018) (dismissing third-party beneficiary claim based on BAA provision).

***Second*, Plaintiffs fail to allege any specific contract was intended to benefit any specific Plaintiff.** If the Court finds Plaintiffs can sufficiently identify the parties and contracts that they believe benefit them (they do not), Plaintiffs allege only that the contracts were "intended to protect patients *like* Plaintiffs[]," not that the contracts were intended to benefit any Plaintiff. CAC ¶ 432 (emphasis added); Appendix C. This is insufficient to plausibly allege that any specific Plaintiff is a third-party beneficiary of any specific BAA, particularly given the presumption against third-party beneficiary status. *See Bruno*, 2024 WL 5305079, at *8 ("All doubts must be resolved against conferring third-party beneficiary status.").[28]

Healthcare Sys., Inc., No. 4:20-cv-00185, 2022 WL 10078122, at *12 (S.D. Ind. Oct. 17, 2022) (internal quotation omitted); *see also* Appendix C.

[28] This claim also fails as to the Non-Change Defendants for the independent reason that Plaintiffs have not plausibly alleged that the Non-Change Defendants entered into any contract with any payor or provider that even *could* have provided any Plaintiff's PI to Change. Even if *Change* is a business associate or sub-business associate to an entity that

***Third*, HIPAA cannot form the basis of a breach of contract claim.** Even if their was a contract here, Plaintiffs cannot allege a breach of any such contract. Plaintiffs rely on alleged violation of HIPAA to assert breach. CAC ¶ 433 ("Defendants violated HIPAA and, thereby, breached [their contracts]."). But as discussed *supra* Section V.A., HIPAA is not enforced through private litigants, and to allow Plaintiffs to bootstrap HIPAA as evidence of breach would subvert this clear legislative intent.

Setting HIPAA aside, Plaintiffs cannot plausibly allege breach of contract for the same reasons they fail to allege breach of duty under negligence: simply alleging that a sophisticated, international criminal hacked Change's system does not mean that any Defendant breached any contractual obligations to their customers, let alone to Plaintiffs. *See* CAC ¶ 433; *see also In re Anthem, Inc. Data Breach Litig.*, No. 14-MD-02617, 2016 WL 3029783, at *20 (N.D. Cal. May 27, 2016).

VIII. PLAINTIFFS' UNJUST ENRICHMENT CLAIM HAS NO MERIT

Plaintiffs' unjust enrichment claim must be dismissed because the claim is precluded as a matter of law under the laws of every state, and Plaintiffs fail to plausibly plead the essential elements of unjust enrichment, namely that any plaintiff conferred a benefit on any Defendant or that Defendants retained any benefit unjustly. *See, e.g.*, *Caldas*, 820 N.W.2d at 838 (discussing unjust enrichment in Minnesota); *see also* Appendix D.

---

serves as a payor or provider to a Plaintiff, Plaintiffs' allegation that "each Defendant must have entered into one or more BAA with one or more covered entities" that provided Plaintiffs' PII to Change, is conclusory and belied by Plaintiffs' allegations about the role of UHG, Optum, Inc., and OptumInsight, Inc. *See* CAC ¶¶ 148-67, 431.

Unjust enrichment is a quasi-contractual remedy that requires "(1) 'a benefit conferred upon the defendant by the plaintiff'; (2) 'appreciation by the defendant of such benefit'; and (3) 'acceptance of such benefit under such circumstances that it would be inequitable for him to retain the benefit without payment of the value thereof.'" *Freeman Indus., LLC v. Eastman Chem. Co.*, 172 S.W.3d 512, 525 (Tenn. 2005) (citation omitted).

A. Unjust Enrichment Is Unavailable to Plaintiffs As a Matter Of Law

Plaintiffs' unjust enrichment claim fails as a matter of law for at least three reasons.

First, six states—California, Georgia, Illinois, Massachusetts, New Jersey, and New York—do not recognize unjust enrichment.[29] *See, e.g.*, *Dias v. Spartan Micro*, Inc., No. 8:22-cv-00834, 2022 WL 17216820, at *7 (C.D. Cal. Sept. 14, 2022) (dismissing claim because "[t]here is no cause of action in California for unjust enrichment."); *see also* Appendix D.

Second, like their contract and negligence *per se* claims, Plaintiffs' unjust enrichment claim cannot be predicated on an allegation of HIPAA non-compliance. CAC ¶ 438 (alleging Defendants benefitted from Plaintiffs' PII, which was obtained "under the promise" of HIPAA compliance). *See supra* Section V.A; *Espinoza v. Gold Cross Servs., Inc.*, 234 P.3d 156, 158-59 (Utah Ct. App. 2010) (upholding dismissal of unjust enrichment claim because court could not enforce HIPAA regulations "either directly or as a

[29] Certain states allow unjust enrichment to proceed even if an adequate remedy at law exists. *See* Appendix D. To the extent the law of any states other than those states is applied to any Plaintiff's unjust enrichment claims, those claims are precluded because an adequate remedy at law exists.

component of a state cause of action"). This failing requires dismissal of the unjust enrichment claim for all Plaintiffs.

Third, unjust enrichment may not proceed when an adequate remedy at law exists, which necessitates dismissal of this claim under the laws of 37 states. *See* Appendix D. Plaintiffs allege tort and contract claims under the laws of *all* states, plus statutory claims in twenty-three states. *See* CAC ¶¶ 397-449 (alleging tort and contract claims), 460-1031 (alleging statutory claims). Thus, Plaintiffs have adequate remedies at law, and Count IV must be dismissed for this independent reason.[30] *See Ahlgren v. Muller*, 438 F. Supp. 3d 981, 990 (D. Minn. 2020) (dismissing unjust enrichment claim because the statutory claim provided an adequate remedy at law); Appendix D.

B. Plaintiffs Fail To Plausibly Plead the Elements of Unjust Enrichment

1. Plaintiffs Fail To Allege They Conferred Any Benefit to Defendants

In data breach litigation, plaintiffs must allege that they paid defendants some amount of money for data security to plead unjust enrichment. *E.g.*, *SuperValu IV*, 925 F.3d at 966 (dismissing unjust enrichment when plaintiff failed to allege he paid a premium for

[30] Some states allow unjust enrichment to be pled in the alternative, at least where no contract exists governing the relationship. *See Buchl v. Gascoyne Materials Handling & Recycling, L.L.C.*, No. 1:17-CV-48, 2018 WL 3259740, at *4 (D.N.D. Mar. 21, 2018). This exception does not apply because (1) Plaintiffs do not plead unjust enrichment in the alternative to their third-party beneficiary breach of contract claim; and (2) Plaintiffs plead that express contracts exist that govern the parties' relationship and those contracts preclude Plaintiffs from obtaining third-party beneficiary status. *See supra* Section V; *see Tahirou v. New Horizon Enters., LLC*, No. 3:20-CV-0281, 2022 WL 596741, at *4 (D. Conn. Feb. 28, 2022) (dismissing claim because it was not pled in the alternative); *Caldas*, 820 N.W. 2d at 839 (holding plaintiffs may not "bring an unjust enrichment claim to avoid the result that they lack third-party beneficiary status to enforce").

data protection); *Irwin v. Jimmy John's Franchise*, 175 F. Supp. 3d. 1064, 1072 (C.D. Ill. 2016) (dismissing unjust enrichment claim under Illinois and Arizona law when plaintiff paid for food but "did not pay for a side order of data security and protection," which "was merely incident to her food purchase"). Nowhere do Plaintiffs allege payment to Defendants, requiring dismissal of the claim as to all Defendants.

Even if the Court were to look past this failure, Plaintiffs also fail to plausibly allege that they conferred any benefit to, or engaged in a bargained-for exchange with, any Defendant. *See, e.g.*, *Caldas*, 820 N.W.2d at 838 (noting plaintiff "must establish an implied-in-law or quasi-contract" with defendant); *see also* Appendix D. The only benefit Plaintiffs allege that Defendants received is personal information provided by healthcare providers or payors to Change. *E.g.*, CAC ¶ 3. But the conferral of personal information fails to qualify as a "benefit" in at least 15 states. *See* Appendix D; *see also In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 592 (N.D. Ill. 2022) (courts routinely reject "that an individual's [PII] has an independent monetary value").

Plaintiffs also do not plausibly allege that they provided their information to any Defendant directly, or in exchange for anything of value from Defendants. Instead, Plaintiffs allege their personal information was provided to Change by medical providers or payors. *See, e.g.*, *id.* ¶ 188. This is insufficient to allege unjust enrichment. *In re MCG Health Data Sec. Issue Litig.*, No. 2:22-CV-849-RSM-DWC, 2023 WL 3057428, at *5-6

(W.D. Wash. Mar. 27, 2023) (dismissing unjust enrichment when plaintiffs' PII was provided to defendant by third-party medical providers and not plaintiffs).[31]

2. Plaintiffs Fail To Plausibly Allege Any Enrichment Was Unjust

Count IV also fails because Defendants did not retain any benefit unjustly. *See, e.g.*, *Freeman*, 172 S.W.3d at 525 ("The most significant requirement of an unjust enrichment claim is that the benefit to the defendant be unjust."); *see also* Appendix D. Plaintiffs' formulaic recitation of the elements is insufficient, *i.e.*, that "Defendants' acceptance of the benefits . . . under the facts and circumstances is unfair, unjust, and inequitable" and that "Defendants should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class members." CAC. ¶¶ 443-44; *see RBG Mgmt. Corp. v. Vill. Super Mkt., Inc.*, 692 F. Supp. 3d 135, 155 (S.D.N.Y. 2023) (dismissing claim for failure to allege "why it is against equity and good conscience to allow [defendant] to retain the alleged benefit") (internal quotation omitted). And while Plaintiffs allege generally that data analytics is the future of healthcare, CAC ¶ 183, and speculate that Defendants profited from certain individuals' de-identified PII, *id.* ¶ 167, even accepted as true, Plaintiffs do not allege: (1) that *their* information benefitted Defendants; or (2) that Plaintiffs were entitled to a share of the alleged profit. There is thus no "monetary benefit" that belongs to Plaintiffs. *Id.* ¶

[31] Plaintiffs summarily allege that they would not have allowed third parties to send their PII to Change if they had known that Change "had not secured their Personal Information or that they used their private medical information for their own financial gain." CAC ¶ 445. Plaintiffs have no control over the complex medical claim payment process. Allegations to the contrary are plainly not well-pleaded, *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009), and are belied by allegations that medical providers continue to send Plaintiffs' PII to Change despite security purportedly remaining inadequate. CAC ¶¶ 453-54.

444; *SuperValu IV*, 925 F.3d at 966. Accordingly, Plaintiffs failed to plausibly plead that Defendants unjustly retained any benefit, and Count IV must be dismissed.

IX. THE DECLARATORY JUDGMENT ACT CLAIM IS DUPLICATIVE AND STATES NO RISK OF IMMINENT AND SUBSTANTIAL HARM

Plaintiffs' claim for declaratory and injunctive relief under the Declaratory Judgment Act ("DJA"), 28 U.S.C. § 2201, should be dismissed for two reasons. *First*, Plaintiffs lack standing to bring a DJA claim because they fail to plausibly allege that the risk of future harm is "imminent and substantial." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 435 (2021); *see also Lochridge v. Quality Temp. Servs., Inc.*, No. 22-cv-12086, 2023 WL 4303577, at *8 (E.D. Mich. June 30, 2023) (dismissing DJA claim for failing to plausibly allege "facts tending to show that a second data breach is currently impending or there is a substantial risk that one will occur"). The Complaint includes only formulaic and conclusory allegations on this point. CAC ¶ 453 (alleging that "Defendants' data security measures remain inadequate"); *id.* ¶ 457 (alleging that the "risk of another data breach is real, immediate, and substantial"). This is plainly insufficient where (1) only Change's systems were impacted, *id.* ¶ 259; (2) Plaintiffs acknowledge that Change has taken steps post-incident to further strengthen cybersecurity, *id.* ¶ 258; and (3) Plaintiffs allege no facts to suggest that UHG, Optum Inc., or OptumInsight, Inc. hold Plaintiffs' information or are at risk of a cyberattack beyond the risk that applies to every organization. *See generally* CAC; *see also Iqbal*, 556 U.S. at 678; *Lochridge*, 2023 WL 4303577, at *8.

Second, the DJA claim is entirely duplicative of and encompassed by Plaintiffs' negligence and negligence *per se* claims and thus serves no "useful purpose." *Fairview*

Health Servs. v. Armed Forces Off. of Royal Embassy of Saudi Arabia, 705 F. Supp. 3d 898, 911-13 (D. Minn. 2023). Indeed, both claims allege the same harm and seek the same relief. *Compare* CAC ¶¶ 414-27 (negligence claims alleging breach of duty under FTCA and HIPAA and seeking an injunction because they allege Defendants data security remains inadequate), *with id.* ¶¶ 453-56 (generally same). Courts regularly dismiss DJA claims when they merely duplicate claims "that will necessarily settle the issues for which the declaratory judgment is sought." *Amusement Indus., Inc. v. Stern*, 693 F. Supp. 2d 301, 311 (S.D.N.Y. 2010) (collecting cases). The Court should do the same here.

X. STATE CONSUMER PROTECTION CLAIMS FAIL AS PLAINTIFFS ARE NOT CONSUMERS, MADE NO PURCHASE, AND DO NOT ALLEGE UNLAWFUL OR UNFAIR CONDUCT OR INTENTIONAL DISCLOSURE

Plaintiffs' state consumer protection statute claims suffer from the same deficiencies—*i.e.*, failure to allege causation, injury, or that any Defendant's cybersecurity practices were unreasonable. *See supra* Sections I, III. Furthermore, these statutes require Plaintiffs to allege facts supporting various elements—*e.g.*, a consumer relationship—that appear nowhere in the Complaint, and they contain numerous restrictions and limitations that require dismissal—*e.g.*, Alabama requires a purchase of goods or services for household use in order to assert a claim under the consumer protection act.[32] Those failings of the CAC, as described below, require dismissal of those claims.

[32] A plaintiff can only assert claims under state statutes where she resides or was injured. *See, e.g.*, *Insulate SB, Inc. v. Advanced Finishing Sys., Inc.*, No. 13-2664, 2014 WL 943224, at *10-11 (D. Minn. Mar. 11, 2014) (*quoting In re Ductile Iron Pipe Fitting Indirect Purchaser Antitrust Litig.*, No. 12-169, 2013 WL 5503308, at *11 (D.N.J. Oct. 2, 2013) ("Named plaintiffs lack standing to assert claims under the laws of the states in which they

A. Plaintiffs Do Not Satisfy Injury and Causation Requirements

All state consumer protection statutes here require Plaintiffs show they have suffered "actual damages," "ascertainable loss of money or property," "actual pecuniary loss," or similar monetary, out-of-pocket harms. *See SuperValu IV*, 925 F.3d at 964-65 (dismissing Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA") claim for failure to allege "actual pecuniary loss"); *see also* Appendix E. As discussed *supra* Section III.A, many Plaintiffs fail to plead fraud that led to unreimbursed costs, or any out-of-pocket harms. For this reason, in data breach cases, courts routinely dismiss state consumer protection claims alleging the types of harm in the CAC, namely (1) increased risk of fraud, *e.g.*, *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752, 2017 WL 3727318, at *22 (N.D. Cal. Aug. 30, 2017) (dismissing UCL claim); (2) mitigation costs and related self-generated expenses, *e.g.*, *Supervalu IV*, 925 F.3d at 964-65 (dismissing ICFA claim); (3) loss of value of personal information, *e.g.*, *In re iPhone Application Litig.*, No. 11-MD-02250, 2011 WL 4403963, at *14 (N.D. Cal. Sept. 20, 2011) (dismissing UCL claim); (4) spam calls, *e.g.*, *Nelson v. Ashford Univ., LLC*, No. 16-cv-3491, 2016 WL 4530325, at *3 (N.D. Ill. Aug. 29, 2016) (dismissing ICFA claim); and (5)

---

do not reside or in which they suffered no injury."). To the extent Plaintiff(s) residing in a particular state fail to allege the elements of that state statute, the claim should be dismissed. *Id.* at *11-12 (dismissing statutory claim where state resident plaintiff failed to adequately plead that claim). Similarly, if the Court agrees that Plaintiffs Agres, Antonio, and Seibert lack Article III standing, Counts XXXVII, XVII, and XXII must be dismissed because they are the only Plaintiffs from those states. *See Hollingsworth v. Perry*, 570 U.S. 693, 715 (2013) (holding lack of Article III standing precluded state statutory claim).

fraud with no out-of-pocket loss, *e.g.*, *SuperValu IV*, 925 F.3d at 964 (dismissing ICFA claim).

Here, too, all Plaintiffs that bring a consumer protection act claim fail to plead an "ascertainable loss of money" or similar harms required to sustain their claims.[33] *See* Appendix E. Certain Plaintiffs attempt to mask this issue by alleging what appears at first blush to be "out-of-pocket losses," e.g., the cost of gas to drive to her bank and the station to file a police report, CAC ¶ 120, but these attenuated, self-generated mitigation costs are insufficient to save Plaintiffs' claims. *See Supervalu IV*, 925 F.3d at 964 ("[T]ime . . . spent protecting [one]self against the threat of future identify theft does not amount to an out-of-pocket loss.").

Plaintiffs also fail to plead causation, an essential element of 21 state consumer protection act claims. *See* Appendix E. For the same reasons discussed *supra* Sections I.B and III.C, their state consumer protection claims should fail.

[33] Plaintiffs Christenson (AL, ¶ 17, Count VI); Dixon (AK, ¶ 19, Count VII), Phillips, (AZ, ¶ 21, Count IX), Jackson (CA, ¶ 25, Count X), Dugan (CO, ¶ 27, Count XIV), Mammad (CT, ¶ 29, Count XV), Antonio (HI, ¶ 43, Count XVII), Leffers (IL, ¶ 47, Count XVIII), M.O. (IL, ¶ 49, Count XVIII), Bonier (LA, ¶ 62, Count XX), Merrill (ME, ¶ 64, Count XXI), Seibert (MD, ¶ 66, Count XXII), Paul (MA, ¶ 68, Count XXIII), Brooks (MN, ¶ 72, Count XXIV), Powers (MN, ¶ 74, Count XXIV), Allen (MN, ¶ 76, Count XXIV), Rubera (NH, ¶ 90, Count XXVI), Schiller (NM, ¶ 96, Count XXIX), Korlou (NY, ¶ 98, Count XXX), Donaldo (NY, ¶ 100, Count XXX), Morgan (NC, ¶ 102, Count XXXI), Lanier (OR, ¶ 112, Count XXXIII), Bussick (RI, ¶ 120, Count XXXIV), Tynch (SC, ¶ 122, Count XXXV), Agres (VT, ¶ 134, Count XXXVII), Ivory (WA, ¶ 138, XXXVIII), and Fossen (WY, ¶ 146, Count XLI).

B. Plaintiffs Are Not Consumers and Made No Purchases from Defendants

Claims under the laws of 13 states must be dismissed because Plaintiffs are not consumers, customers, or purchasers as required, nor have they pled any consumer relationship with Defendants.[34] *See, e.g.*, *ALK 2, LLC v. K2 Marine, Inc.*, 647 F. Supp. 3d 1253, 1260-61 (M.D. Ala. 2022) (dismissing Alabama Deceptive Trade Practices Act claim because plaintiff was not a "consumer," or "natural person who buys goods or services for personal, family, or household use" from defendant); *see also* Appendix E. Nor could they. As alleged, Change facilitates communications between healthcare providers and payors, CAC ¶ 187. Plaintiffs do not allege that they paid Defendants for any services or that they chose to use any Defendants' services at all. *See generally* CAC ¶¶ 17-147.[35]

C. Plaintiffs Failed to Satisfy Statutory Notice Requirements

Plaintiff Jackson's California Consumer Privacy Act ("CCPA") claim must be dismissed for failure to provide pre-suit notice. Cal. Civ. Code § 1798.150(b) (requiring 30-days' written notice prior to initiating suit); *Griffey v. Magellan Health Inc.*, No. CV-20-01282-PHX-MTL, 2022 WL 1811165, at *6 (D. Ariz. June 2, 2022) (dismissing with prejudice CCPA claim brought three days after plaintiff first served defendant with notice).

[34] Counts VI, VII, IX, XIV, XVII, XVIII, XXI, XXII, XXX, XXXI, XXXIV, XXXVII, and XLI.

[35] Similarly, Arizona Consumer Fraud Act (Count IX) requires the sale of merchandise. *See, e.g.*, *Cellco P'ship v. Hope*, No. CV11-0432 PHX, 2011 WL 3159172, at *6-7 (D. Ariz. July 26, 2011) (dismissing Arizona CFA claim because defendant was not "buyer in the merchandise transaction"); *see also* Appendix E. Plaintiff Phillips makes no allegation that any Defendant sold her any merchandise, and her claim must be dismissed. *See* CAC ¶¶ 21; *see also* Appendix E.

Likewise, Plaintiff Paul's Massachusetts Consumer Protection Act claim must be dismissed for failure to provide pre-suit notice. *See Rodi v. S. New Eng. Sch. of L.*, 389 F.3d 5, 19 (1st Cir. 2004) (dismissing ch. 93A claim where pleading failed to state that plaintiff complied with pre-suit notice requirement); Appendix E. Demand letters that fail to specifically identify the plaintiff and their specific injuries do not suffice. *See Alberts v. Payless Shoesource, Inc.*, No. 13-12262, 2014 WL 4924243, at *1 (D. Mass. Sept. 29, 2014) (dismissing ch. 93A claim where demand letter referred to "plaintiff" but not by name). No Plaintiff alleges that they sent a pre-suit demand letter to Defendants. *See generally* CAC ¶¶ 17-147. Accordingly, Counts XIII, XXIII, and XLI should be dismissed. *See* Appendix E.

D. Plaintiffs Seek Relief Beyond What Is Authorized By Statutes

Certain state statutes prohibit Plaintiffs from seeking damages or class-wide relief, and California's statute excludes data covered by HIPAA. Plaintiffs Jackson, Brooks, Powers, and Allen seek economic damages across all of their consumer protection claims, but the applicable statutes in their respective states limit claims to, at most, injunctive relief. *See Gisairo v. Lenovo (United States) Inc.*, 516 F. Supp. 3d 880, 890 (D. Minn. 2021) ("the sole remedy under Minnesota Deceptive Trade Practices Act the is injunctive relief"); *Madrid v. Perot Sys. Corp*., 130 Cal. App. 4th 440, 445 (Cal. Ct. App. 3d 2005) ("damages are not recoverable under the California Unfair Competition Law"). Counts X (California) and XXIV (Minnesota) should thus be dismissed to the extent Plaintiffs seek monetary relief. *See* CAC ¶ 535 (seeking economic damages); ¶ 763 (same); *see also* Appendix E.

Alabama, Louisiana, and South Carolina also preclude class-wide relief. *In re Ford Motor Co. F-150 & Ranger Truck Fuel Econ. Mktg. and Sales Pracs. Litig.*, No. 2:19-md-02901, 2022 WL 551221, at *19 (E.D. Mich. Feb. 23, 2022) (dismissing Alabama, Louisiana, and South Carolina consumer protection act claims because they cannot be pursued on a representative basis). To the extent Plaintiffs intend to bring Counts VI, XX, and XXXV on behalf of putative classes, they must be dismissed. *See* Appendix E.

Finally, Count XIII (CCPA) does not apply to HIPAA-regulated data or entities. Cal. Civ. Code §§ 1798.145(c)(1)(A)-(B); *see Tate v. EyeMed Vision Care, LLC*, No. 1:21-cv-36, 2023 WL 6384367, at *10 (S.D. Oh. Sept. 29, 2023) (dismissing CCPA claim related to HIPAA-regulated data). Plaintiffs allege the Cyberattack affected California Plaintiffs' "protected health information" under HIPAA, requiring dismissal of Count XIII. CAC ¶ 1.

E. Defendants Did Not Engage in Unlawful or Unfair Conduct

Like their negligence strict liability framing, Plaintiffs' consumer protection act claims suggest that because the Cyberattack occurred, each Defendant must have engaged in "unlawful" or "unfair" business practices by failing to "secure" PII from access by a sophisticated threat actor. Not so, and Plaintiffs cannot point to any other acts to sufficiently allege that Defendants acted "unlawfully" or "unfairly" under the statutes.[36]

[36] Most consumer protection statutes offer three distinct theories of liability, for: (1) "unlawful"; (2) "unfair"; or (3) "fraudulent" or "deceptive" conduct. *See, e.g.*, *S. Bay Chevrolet v. Gen. Motors Acceptance Corp.*, 72 Cal. App. 4th 861 (1999) (discussing each prong of the California UCL). Plaintiffs generally have not alleged "fraudulent" or "deceptive" conduct, and instead rely on the "unfair" or "unlawful" theories. *See, e.g.*, CAC ¶ 472 (alleging "unlawful and unfair business practices"). Counts XXX (New York) and XXXVII (Vermont) are the only counts that allege Defendants engaged in "deceptive

1. No Unlawful Conduct Under HIPAA, FTC Act, or Other Statutes

Plaintiffs reference numerous statutes as the basis for Defendants' alleged "unlawful" conduct. To the extent their claims rely on alleged incompliance with the FTC Act and HIPAA, those efforts fail. Putting aside an inability to show a violation of any duty related to data security, *see supra* Section V.C, Plaintiffs' claims cannot be predicated on these laws because they preclude private enforcement. *See supra* Section V.A; *Fero v. Excellus Health Plan, Inc.,* 236 F. Supp. 3d 735, 777 (W.D.N.Y. 2017) (dismissing NY Gen. Bus. L. § 349 claim because it could not be predicated on violations of HIPAA or the FTC Act, which do not have private rights of action). The Court should not allow Plaintiffs to circumvent these remedial schemes and "thwart" legislative intent through consumer protection statutes. *Broder v. Cablevision Sys. Corp.*, 418 F.3d 187, 199 (2d Cir. 2005).

Count XXII also alleges Defendants violated the Maryland Social Security Number Privacy Act, Md. Code Ann. Comm. L. § 14-3401, *et seq*., CAC ¶ 708, but this law lacks a private right of action too. *CarMax Auto Superstores Inc. v. Sibley*, 194 F. Supp. 3d 392, 402 (D. Md. 2016). Plus it requires a defendant to "post," "print," or "initiate the

---

acts" and that Plaintiffs were "deceived." *Id.* ¶¶ 850-51, 969. To the extent Plaintiffs attempt to bring a claim under a fraudulent or deceptive prong of New York, Vermont, or any other state act, the claim fails. Plaintiffs do not identify any "deceptive" acts or omissions and therefore cannot meet the heightened pleading standards of Rule 9(b). Furthermore, any claim of "deceptive" conduct fails because Plaintiffs do not plead that they viewed, were exposed to, or were aware of any Defendant's statements, let alone that they relied on them. *See Troy v. Am. Bar Ass'n*, No. 23-CV-03053, 2024 WL 1886753, at *6 (E.D.N.Y. Apr. 30, 2024) (dismissing N.Y. Gen. Bus. Law §349 claim for failing to allege Plaintiffs saw allegedly misleading privacy policy); *Bergman v. Spruce Peak Realty, LLC*, 847 F.Supp.2d 653, 671-73 (D. Vt. 2012) (dismissing Vermont Consumer Fraud Act claim for failing to allege that statements affected plaintiff's decision to purchase product).

transmission," of an SSN, Md. Code Ann. Comm. L. §§ 14-3402(a)(1), (2), (4), and Plaintiff Seibert does not allege these affirmative acts. *See* CAC ¶¶ 66, 706-26.

Count X (UCL) also alleges violations of the CCPA and California Customer Records Act, CAC ¶¶ 521, 524, which fails for the reasons articulated in Sections X.C, *supra*, and XI, *infra*. Counts XV, XVIII, XX, XXII, and XXVIII reference violations of their respective state data breach notification laws, CAC ¶¶ 601, 642, 671, 709, 815, but as discussed in Section XI, *infra*, Plaintiffs fail to plead any unreasonable delay in notice or any injury resulting from a delay. Counts XVIII, XXII, XXIII, XXVII, and XXXII allege violations of statutes requiring reasonable data security, but as discussed *supra* Section III, Plaintiffs fail to plead that Defendants had unreasonable data security. These claims must be dismissed.

2. Plaintiffs Have Not Shown Egregious or Aggravating Circumstances

Plaintiffs' state consumer protection act claims also fail because their allegations of "unfair practices" require "egregious," "aggravating," or similarly "immoral" behavior, which Plaintiffs cannot and do not plausibly allege. *See, e.g.*, *Walker v. Hixson Autoplex of Monroe, L.L.C.*, 240 So. 3d 1088, 1095 (La. Ct. App. 2017). Plaintiffs rely on what Defendants purportedly learned about the threat actor's methods after the attack to suggest that Defendants' pre-cyberattack behavior *must* have been unreasonable or contrary to industry standards. This theory would mean every cyberattack victim would be in violation of every state consumer protection statute once they understood *post hoc* an incident's cause. That is not the law. *See, e.g.*, *In re MCG Health Data Sec. Issue Litig.*, No. 2:22-cv-849, 2023 WL 3057428, at *14 (W.D. Wash. Mar. 27, 2023) (dismissing Louisiana Unfair

Trade Practices Act unfairness prong claim because "conclusory allegations that, because of the data breach, [Defendant] did not implement and maintain adequate data security" were insufficient), *R. & R. adopted* 2023 WL 4131746 (W.D. Wash. June 22, 2023).

Furthermore, "courts have declined to find 'highly offensive' conduct of an 'egregious breach of social norms' where only negligence is alleged with respect to a data breach, as opposed to intentional violations of privacy rights." *In re Accellion, Inc. Data Breach Litig.*, 713 F. Supp. 3d 623, 646-47 (N.D. Cal. 2024) (collecting cases). Nowhere do Plaintiffs allege an intentional or even reckless release of their information; to the contrary, they allege the sophisticated threat actor BlackCat stole information from Change's system. CAC ¶¶ 251-61. Plaintiffs claim that Defendants stored data in a "knowingly unsafe and unsecured manner," *e.g.*, *id.* ¶ 463, but this speculative allegation and attempt to suppose pre-Cyberattack knowledge based on post-Cyberattack learnings is insufficient. Allegations of inadequate oversight or purportedly deficient data security are far from the intentionality required for "highly offensive" conduct required to establish an unfairness consumer protection claim. *In re Accellion*, 713 F. Supp. 3d at 646.

Plaintiffs cannot plausibly allege that Defendants violated a single state or federal statute or that Defendants' actions were "unfair" because they were targeted and attacked by a sophisticated threat actor. All state consumer protection claims must be dismissed.

F. Plaintiffs Cannot Satisfy the Requirements of Medical Information Statutes

1. There Is No Intentional Disclosure of Medical Information Under California Confidentiality of Medical Information Act ("CMIA") (Count XII)

Plaintiff Jackson's allegations do not support a CMIA claim, which requires an intentional disclosure of medical information. *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, No. 19-md-2904, 2021 WL 5937742, at *33-34 (D.N.J. Dec. 16, 2021) (dismissing CMIA claim for failure to allege any intentional disclosure of "medical information," which is defined as "individually identifiable information … regarding a patient's medical history, mental or physical condition, or treatment") (internal quotations omitted). Plaintiff must allege an "affirmative communicative act" by each Defendant demonstrating an intent to disclose medical information. *See, e.g.*, *Sutter Health v. Super. Ct. Sacramento Cnty.*, 174 Cal. Rptr., 3d 653, 661 (Cal. Ct. App. 2014) (dismissing CMIA claim in data breach case in part because no affirmative disclosure occurs when information is stolen). Indeed, Plaintiff pled the opposite—that "[v]arious cybercriminals . . . accessed and obtained California Plaintiffs' and California Subclass Members' personal medical information . . . ." *See* CAC ¶ 557.[37]

Plaintiff Jackson also fails to allege that Change had possession of any of her medical information, and she certainly does not allege that any Defendant intentionally disclosed her medical information. *Id.* ¶¶ 25-26. Even read in the light most favorable to Plaintiff Jackson, she alleges that on an undefined date, she received notice that her

[37] The Court need not credit implausible allegations. *See Iqbal*, 556 U.S. at 682.

"information was found on the dark web," but not that her "medical information" was available, or that it was "disclosed" by any Defendant. *Id.* To the extent Plaintiff Jackson seeks to hitch her CMIA claim to putative class members whose "medical information" may have been impacted, her claim fails. *See Spokeo*, 578 U.S. at 338 n.6 ("[E]ven named plaintiffs who represent a class must allege and show that they personally have been injured.") (internal quotations omitted). Count XII thus must be dismissed.

2. The Minnesota Health Records Act ("MHRA") (Count XXV) Claim Fails Because Plaintiffs Do Not Allege A Release of Health Records

The Minnesota Plaintiffs fail to allege that any Defendant possessed their "health records," defined as "any information…that relates to the…physical or mental health or condition of a patient; the provision of healthcare to a patient; or the…payment for the provision of healthcare to a patient."[38] Minn. Stat. Ann. § 144.291 subdiv. 2(c). More critically, the Minnesota Plaintiffs do not allege an affirmative "release" of records, *i.e.*, to "set free from or let go or to make available for use." *Larson v. Nw. Mut. Life Ins. Co.*, 855 N.W.2d 293, 302 (Minn. 2014) (internal quotations and alterations omitted). Minnesota Instead, they allege that "[v]ia the Data Breach, Defendants released" Plaintiffs' PII, which is insufficient. *See* CAC ¶ 769; *In re Netgain Tech. LLC*, *Customer Data Breach Litig.*, No. 21-cv-1210 (SRN/LIB), 2022 WL 1810606, at *16 (D. Minn. June 2, 2022) (dismissing MHRA in breach case because "a stealing does not constitute an affirmative release").

[38] To the extent all Plaintiffs seek to bring Count XXV, it should be dismissed as to all non-Minnesota-resident Plaintiffs. *See Insulate SB, Inc.*, 2014 WL 943224, at *10-11.

3. The Wisconsin Health Care Records Law ("WHCRL") (Count XL) Claim Fails As Plaintiff Cannot Allege Disclosure or Resulting Harm

WHCRL prohibits the negligent disclosure of "patient health care records," Wis. Stat. §§ 146.82(1), 146.84(1)(bm). This law applies only to actual records, not information associated with or derived from those records. *See, e.g.*, *Mosley v. Oakwood Lutheran Senior Ministries*, No. 2022AP907, 2023 WL 4782874, at *4-6 (Wis. Ct. App. July 27, 2023) (dismissing claim under Wis. Stat. § 146.84(1)(bm) where plaintiff alleged test results were released, but not underlying healthcare records). Plaintiff Anderson has not alleged that any Defendant had possession of, or negligently disclosed, his "health care records," defined by Wis. Stat. § 146.81(4) as "all records related to the health of a patient prepared by or under the supervision of a health care provider . . . [and] billing statements and invoices for treatment or services provided by a health care provider." Even if Plaintiff Anderson alleged a negligent disclosure of his healthcare records, WHCRL requires that the disclosure cause injury. *Id.* § 146.84(1)(bm). Plaintiff Anderson does not allege any harms that could possibly be related to the exposure of his health records. CAC ¶ 144 (alleging an increase in spam messages and unauthorized access to his vehicle insurance and satellite radio accounts). Count XL must be dismissed accordingly.

XI. DATA BREACH NOTIFICATION CLAIMS FAIL BECAUSE PLAINTIFFS DO NOT ALLEGE UNREASONABLE DELAY OR HARM

The state data breach notification laws ("Notice Claims") fail because: (1) Georgia does not provide a private right of action; (2) Plaintiffs are not "consumers," as required by California, New Jersey, and North Carolina laws; and (3) Plaintiffs fail to adequately allege that notification was unreasonably delayed. In addition, all Plaintiffs allege they

received a Notice of Data Breach letter from Change, no Plaintiff alleges any injury (or "actual damages") sustained by any delay in receiving notice, and no Plaintiff plausibly alleges that any Non-Change Defendant owed them notice of the cyberattack *on Change*.[39]

First, Count XVI must be dismissed because the Georgia Identity Theft Protection Act has no private right of action, *see Manley v. Experian Data*, No. 4:21-cv-00199, 2021 WL 9274364, at *2 (N.D. Ga. Dec. 13, 2021), and applies only to "information brokers" (e.g., credit bureaus), and thus does not apply here. Ga. Code Ann. § 10-1-910 (2024).[40]

Second, the California, New Jersey, and North Carolina Notice Claims should be dismissed because Plaintiffs Loforese, Sack, Morgan, and Jackson can only enforce those claims under their state consumer protection laws if they are "consumers," which they have not alleged. *Id*. As discussed in Section X.B and by the CAC's own admission that Plaintiffs "had no direct relationship with Change," Plaintiffs cannot state a claim under those laws. CAC ¶¶ 545, 820. *See Miller v. NextGen Healthcare, Inc*., 742 F. Supp. 3d 1304, 1332 (N.D. Ga. 2024) (dismissing New Jersey claim where plaintiffs did not "purchase a product for consumption"); *see also* Appendix F.

Third, the Notice Claims should be dismissed for failure to plausibly allege that notice was unreasonably delayed. CAC ¶¶ 497, 546, 621, 664, 799, 821, 888, 959, 1004. Statutory notice requirements are flexible and, in most cases, expressly allow for

[39] Plaintiffs again collectively plead that "Defendants" owed notice, *see* CAC ¶ 956, but the entity "maintaining" the PII, or the "owner or licensee of the information," is responsible for providing notice owed. *See, e.g.*, S.C. Code Ann. § 39-1-90(B).
[40] The Louisiana and Alaska Notice Claims also lack a private right of action for injunctive relief and should be dismissed to the extent they seek that remedy. See Appendix F.

reasonable time to determine the scope of the incident and restore systems. *See* Appendix F. Plaintiffs fail to allege any facts suggesting unreasonable notification timing under these circumstances, which required massive efforts to mail notice to the impacted population, CAC ¶ 544, pursuant to direction from Change's customers. *Id.* ¶ 269, n.130. Notice often takes months after a cyberattack where, as here, third parties must make notice determinations, not the cyberattack victim. *See* CAC ¶ 203, n.67. Indeed, Plaintiffs acknowledge the challenges Change faced: Change also was "prioritiz[ing] rebuilding the Change Platform," CAC ¶ 441, and restoring services, *see, e.g.*, Provider CAC ¶ 5. Because notice was not unreasonably delayed, nearly all of the Notice Claims must be dismissed.[41]

Fourth, for the same reasons described above regarding Plaintiffs' negligence-based failure to timely notify theory, the Notice Claims must be dismissed because Plaintiffs fail to allege injuries tied to any delay in notice, or purported harms that they could have prevented had they been notified sooner. *See* Appendix E; *see also e.g.*, *MCNA* Order, at 22 (dismissing claim because plaintiffs failed to allege harm from untimely disclosure and "it is insufficient to merely allege harm stemming from the breach"). For example, Plaintiff Loforese alleges unauthorized credit card charge *after* he received notice, which could not result from delay in notification. CAC ¶ 92. *Rogers v. Keffer, Inc.*, 243 F. Supp. 3d 650, 663 (E.D.N.C. 2017) (dismissing North Carolina claim for allege no injury from delay).

[41] Counts VIII, XI, XVI, XXVII, XXVIII, XXXII, XXXVI, and XXXIX. Plaintiffs Jackson, Darby, Bonier, and Tynch also fail to allege any specific content that was inaccurate or statutorily required but omitted. CAC ¶¶ 547, 622, 665, 960.

Finally, Plaintiffs cannot, as a matter of law, plausibly allege Notice Claims against the Non-Change Defendants. Plaintiffs broadly allege that "Defendants" owed them notice of the cyberattack on Change. CAC ¶¶ 494, 538-41, 617-18; 660; 795; 817-18; 889; 954-56; 1004. But notice is owed only by Change (the victim), or its customers (entities that provided PII). *See, e.g.*, Alaska Stat. §§ 45.48.010, 45.48.070; Cal. Civ. Code §§ 1798.82(a)-(b); S.C. Code Ann. §§ 39-1-90(A)-(B); Wash. Rev. Code § 19.255.010(1)-(2) (2020). The Non-Change Defendants do not fall into either bucket. To the extent any Notice Claim proceeds, it should be dismissed at least as to the Non-Change Defendants.

CONCLUSION

For all the foregoing reasons, Defendants respectfully request that the Court grant its motion to dismiss Plaintiffs' claims.

Respectfully submitted,

Dated: March 21, 2025

/s/ Allison M. Ryan
Allison M. Ryan
Alicia J. Paller (MN No. 0397780)
Joseph J. Cavanaugh
HOGAN LOVELLS US LLP
555 13th Street NW
Washington, DC 20004
Tel: (202) 637-5600
Fax: (202) 637-5910
allison.holt-ryan@hogbanlovells.com
alicia.paller@hoganlovells.com
joe.cavanaugh@hoganlovells.com

/s/ Peter H. Walsh
Peter H. Walsh (MN No. 0388672)
HOGAN LOVELLS US LLP
80 South Eighth Street, Suite 1225

Minneapolis, MN 55402
Tel: (612) 402-3017
Fax: (612) 339-5167
peter.walsh@hoganlovells.com

Vassi Iliadis
HOGAN LOVELLS US LLP
1999 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Vassi.iliadis@hoganlovells.com
Tel: (310) 785-4727
Fax: (310) 785-4601

Attorneys for Defendants